Evaluación de la regulación y de las herramientas tecnológicas de interceptación telefónica y su impacto a la seguridad nacional en Colombia

Ing. Hernando Piracoca Piracoca

Universidad Nacional de Colombia

Departamento de Ingeniería de Sistemas e Industrial

Bogotá, Colombia

Evaluación de la regulación y de las herramientas tecnológicas de interceptación telefónica y su impacto a la seguridad nacional en Colombia

Ing. Hernando Piracoca Piracoca

Tesis presentada como requisito parcial para optar al título de:
Magister en Ingeniería de Telecomunicaciones

Director
PhD. Mauro Flórez Calderón

Línea de Investigación:
Regulación y Políticas de Telecomunicaciones

Universidad Nacional de Colombia
Facultad de Ingeniería
Bogotá D.C. Colombia
2016

Dedicatoria

A DIOS, Ser supremo, por permitirme vivir para realizar y alcanzar esta meta.

A mi madre, María Hercilia, por darme la vida y enseñarme que los sueños siempre son posibles, si se forjan en la disciplina, el compromiso y la dedicación.

A mis hijos, Mónica, Angie y Camilo, por su apoyo y comprensión de cada día, quienes con su voz de aliento nunca dejaron que mis fuerzas se agotaran, al tiempo que comprendieron que todos esos días dejados de compartir con ellos para dedicarlos a lo académico, eran necesarios para alcanzar nuevas oportunidades y así poder guiarles con mejor criterio en un mundo cada vez más difícil pero que a base de esfuerzo, y sin nunca dejar de soñar, se puede llegar a donde nos lo propongamos.

A mi familia, por su apoyo permanente, quienes nunca dejaron de incentivarme en esos días en que parecía faltaban las fuerzas y la voluntad para continuar

Agradecimientos

Agradezco en primer lugar al Doctor Mauro Flórez Calderón, director de la tesis, Por su gran aporte en el desarrollo del tema de estudio aquí presentado. Gracias a su visión y conocimiento global de las políticas sectoriales; me oriento y guio durante el tiempo de formación en la Maestría, en cada uno de los temas más importantes del sector de las telecomunicaciones, así como en el tema aquí desarrollado, con el cual se logra establecer la necesidad que se tiene en el país en temas de Ciberseguridad y Ciberdefensa.

También agradezco a Mis docentes de la Universidad Nacional de Colombia, en especial a la Dra. Zoila Ramos, quien desde el inicio del estudio del tema, me oriento y dio las recomendaciones para desarrollar una buena metodología de investigación, la cual posteriormente aplique en el desarrollo de la tesis, de la misma forma, me animó en los momentos difíciles haciendo que tuviese la confianza necesaria y que debía alcanzar los objetivos propuesta.

Gracias a la Universidad Nacional de Colombia, donde tuve la oportunidad de realizar mis estudios de Maestría, concediéndome los espacios y apoyos necesarios para desarrollar cada una de las actividades académicas, es el caso de la participación en el simposio de las Tics en Quito Ecuador, siendo esto posible por el apoyo económico dado por la Universidad. Esta participación me permitió tener una visión real y global, acerca del tema de seguridad en comunicaciones, siendo este un insumo importante para la tesis.

Quiero agradecer también a la Policía Nacional de Colombia, y a cada uno de los funcionarios que me permitieron conocer acerca del proceso de interceptación telefónica, y a su vez me suministraron información legal y oportuna, que dadas la dificultad que implicaba este tema, Hizo posible desarrollar los objetivos propuestos.

Resumen

Sin lugar a dudas, uno de los hechos que ha afectado, de una forma u otra, la sociedad, las instituciones de seguridad del estado, y algunas políticas de estado, es el tema de la "Interceptación telefónica", llamada, en medios de comunicación, como las "chuzadas". Al revisar su estado del arte, se observa que esta práctica, data desde antes de la primera guerra mundial, fue usada como una estrategia de guerra, y de inteligencia en lo militar, comercial, etc. Siempre con fines específicos, como conocer lo que se planea hacer por parte de determinadas personas, entidades, grupos, organizaciones etc.

La interceptación telefónica, resulta de suma importancia cuando se vulneran derechos humanos, como el de la libre expresión, derecho a la privacidad, entre otros. Estos derechos son protegidos por convenios internacionales, o las determinadas constituciones de cada país, como ocurre en Colombia. Sin embargo, a través del estudio, se encuentra que también es un procedimiento necesario, como herramienta tecnológica, para salvaguardar la seguridad de las personas, entidades, y en lo general, el estado.

Así, la información es un recurso de alto valor, objeto de la interceptación. Por esta razón cuando la información es vulnerable, resultan consecuencias positivas o negativas, dependiendo los alcances que se den al manejo de esta. Entonces, con el propósito de mejorar cada vez más esta técnica, se han desarrollado tecnologías cada vez más avanzadas, que permitan realizar un control por parte de varios países como: España, Estados Unidos, Francia, Inglaterra, Israel, quienes a su vez venden y comparten sus tecnologías con otros países, como Colombia.

Por otra parte, la regulación en materia de interceptación telefónica, ha tenido su evolución, existiendo tratados y convenios internacionales que la regulan. Aun así, se observa que las normas en general no son homogéneas, por consiguiente, cada país legisla, y en algunos casos, acepta los tratados y convenios internacionales. En el caso Colombiano, se han acogido distintos convenios y tratados, pero al revisar la normatividad, hay profundas diferencias que no reconocen sentencias vitales en la observancia de estas normas, encontrándose diferencias en tiempo entre el avance tecnológico, y las normas, debido, precisamente, al trámite que deben tener las normas para su aprobación.

Palabras clave: Interceptación telefónica, Vigilancia tecnológica, Regulación de Telecomunicaciones, Tecnologías de interceptación telefónica, Información, seguridad.

Multidiciplinarias: 1) Derechos humanos, 2) Riesgos

Abstract

Undoubtedly, one of the facts that has affected, in one way or another, society, institutions of state security, and some state policies, is the subject of "wiretapping", named in media communication, such as "wiretapping". In reviewing the state of the art, it is observed that this practice, given before the First World War was used as a war strategy and intelligence in military, commercial, etc. Always with specific purposes, such as knowing what is planned by certain persons, entities, groups and organizations.

Wiretapping, is extremely important when human rights are broken, such as freedom of expression, right to privacy, among others. These rights are protected by international conventions, or certain constitutions of each country, as in Colombia. However, through the study, it is that it is also a necessary procedure, as a technological tool to safeguard the security of persons, entities, and generally the state.

Thus, information is a resource of high value, subject to interception. For this reason when information is vulnerable, are positive or negative consequences, depending on the scope to be given to the management of this. So in order to constantly improve this technique, we have developed increasingly advanced technologies that allow for control by several countries: Spain, United States, France, England, Israel, who in turn sell and share their technologies with other countries, such as Colombia.

Moreover, the regulation on wiretapping, has had its evolution, existing international treaties and conventions that regulate it. Still, it is observed that the rules in general are not homogeneous, therefore each country legislates, and in some cases, accepts international treaties and conventions. In the case of Colombia, they have received various conventions and treaties, but in reviewing the regulations, there are profound differences that do not recognize life sentences in the observance of these standards, differing in time between technological progress, and standards, precisely because , the procedure that should have standards for approval.Keywords: Wiretapping, surveillance technology,

Telecommunications Regulation, wiretapping technologies, Information security.Multidisciplinary: 1. Human Rights 2. Risks.

Tabla de contenido

Lista de figuras

Lista de tablas

Lista de Símbolos y abreviaturas

	Abreviatura	Término
1	CALEA	Commission on Accreditation for Law Enforcement Agencies
2	CEDH	Convenio Europeo para la protección de los Derechos Humanos
3	CEE	Comunidad Económica Europea
4	CIDH	Comisión Interamericana de Derechos Humanos
5	CIDHH	Corte Interamericana de Derechos Humanos
6	CPP	Código de Procedimiento Penal
7	DAS	Departamento Administrativo de Seguridad
8	DEA	Drug Enforcement Administration
9	DIASE	Dirección Antisecuestro y Extorsión
10	DIJIN	Dirección de Investigación Criminal INTERPOL
11	DIPOL	Dirección de Inteligencia y contrainteligencia de la Policía Nacional
12	ETSI	European Telecommunications Standards Institute
13	FBI	Federal Bureau of Investigation
14	FGN	Fiscalía General de la Nación
15	GSM	Global System for Mobile Communications
16	IMEI	International Mobile Equipment Identity
17	IMSI	Internacional Mobile Subscriber Identity
18	INPEC	Instituto Nacional Penitenciario y Carcelario

19	ISO		International Organization for Standardization
	20	NGN	Next Generation Networks
	21	NSA	National Security Agency
	22	OCDE	Organización para la Cooperación y el Desarrollo Económico
	23	OTAN	Organización del tratado del Atlántico Norte
	24	PCS	Servicios de Comunicación Personal
	25	PUMA	Plataforma Única de Monitoreo y Análisis
	26	RAEES	Residuos de aparatos eléctricos y electrónicos
	27	RCS	Remote Control System
	28	SIGD	Sistema Integral de Grabación Digital
	29	SIJIN	Seccional de Investigación Criminal
	30	SIJINES	Seccionales de Inteligencia y Policía Judicial
	31	SITEL	Sistema Integrado de Interceptación Telefónica
	32	TIC`s	Tecnologías de la Información y las Comunicaciones
	33	TMC	Telefonía Móvil Celular
	34	TSP	Team Software Process
	35	UIAF	Unidad de Información y Análisis Financiero
	36	UIT	Unión Internacional de Telecomunicaciones
	37	VPN	Virtual Private Networ

Introducción

El uso de herramientas tecnológicas con el fin de contrarrestar hechos punibles, es una tendencia cada vez mayor en el mundo. La interceptación telefónica, es el tema de estudio de este trabajo, su importancia radica en el alto impacto que ha llegado a ocasionar en la sociedad, a tal punto que ha implicado la reforma de leyes, cierre de instituciones del estado, escándalos a nivel mundial, entre otros.

En Colombia, la interceptación telefónica ha marcado en la última década, una tendencia en medios de comunicación, casos judiciales, escándalos y en fin una serie de hechos, que controvertidos o no, hacen uso de las tecnologías para interceptar llamadas telefónicas. Al mismo tiempo el mundo ha vivido una serie de acontecimientos que justifican el uso de esta herramienta. Desde el 11 de septiembre del 2001, el mundo cambio su visión en temas de seguridad, este hecho de terrorismo dio un vuelco en materia regulatoria, dando lugar a la Ley Patriot [1], mediante la cual se concede una serie de prioridades a los organismos de seguridad de los Estados Unidos para interceptar comunicaciones en cualquier parte del mundo donde se evidencie un riesgo para la seguridad de los Estados Unidos.

Este tipo de regulación marca la pauta para que los países generen la normatividad que reglamenta el procedimiento de interceptación. En el Caso Colombiano, antes del 2010 no se tiene una normatividad específica, excepto la Constitución política de Colombia y el Código de procedimiento penal, que definen la interceptación telefónica. Dada la importancia que tiene el tema, se hace indispensable estudiarlo y conocer tanto la regulación como las tecnologías que se usan.

Por esa razón se inicia este trabajo con un grupo de funcionarios de una entidad de seguridad del Estado, entonces se realiza un estudio juicioso a fin de elaborar una propuesta regulatoria que satisfaga la necesidad que tiene el País en materia de interceptación. Se llega a la propuesta descrita en el capítulo cinco (5), resultado del estudio de la normatividad internacional y Nacional, obteniendo como validación del tema de estudio, el aporte para realizar la modificación a la legislación colombiana, en sus artículos 235 y 236 del código de procedimiento penal. Al mismo tiempo ante la solicitud por parte de la entidad y la situación que vivía el país a finales de 2010, Se expide el Decreto 1704 [2] del 15 de Agosto de 2012, en el cual este trabajo también tuvo sus aportes. Por último, en la ley 1621, ley de inteligencia, el artículo 44 toma de alguna forma lo propuesto del Art 9, de la propuesta.

Finalmente, se presenta el aporte al proceso de interceptación telefónica, que consiste en estudiar y analizar los riesgos que tiene el proceso, descrito en este documento, el resultado de ello es que hay un estado crítico de ocurrencia del Riesgo “Interceptación ilegal de comunicaciones”, el cual se presenta por diferentes factores como se indica. De esta forma la tesis da alcance a los objetivos propuestos, y hace aportes reales al proceso, toda vez que en el caso de los riesgos, es un trabajo adelantado al interior de una de las unidades que realiza el “Control” del proceso en la entidad, donde queda ya visualizado y seguramente será retomado el estudio para realizar las mejoras al proceso.

1. Estudio de las normas regulatorias de interceptación telefónica

El estudio de las normas regulatorias de interceptación telefónica, es un objetivo de esta tesis, el cual implica en primera instancia establecer el estado del arte de la interceptación telefónica, que permita comprender su entorno y las razones de su implementación y adopción como herramienta estratégica para combatir el crimen organizado por algunos países en el mundo. Los avances tecnológicos a los que se ha llegado hoy en el desarrollo de diversas tecnologías, permiten que los organismos de seguridad del estado en el caso colombiano, las adquieran e implementen con el objeto de asegurar la vida honra y bienes de los ciudadanos. Sin embargo como se demostrará en el desarrollo del trabajo, estas herramientas; no siempre son bien utilizadas, entonces aparecen riesgos que vulneran y atentan contra el mismo ciudadano, en sus derechos humanos. En consecuencia es importante definir de qué forma la regulación y las normas sobre esta materia, por una parte deben permitir y garantizar el desarrollo y uso de las tecnologías de interceptación en beneficio de la sociedad y por otra evitar sus excesos y la afectación de derechos humanos.

1.1. Estado de arte de la interceptación telefónica

La seguridad, se ha constituido a través de la historia en un fundamento muy importante de cualquier tipo de transacción, sea política, económica o social o de otra naturaleza. Indudablemente esta es una preocupación muy vieja. Nicolás Maquiavelo (1469 – 1527) vinculó el tema de la seguridad al ejercicio del poder y a las armas, y su fundamento teórico y político se encuentra en el siglo XVII con el surgimiento del estado Nación”[1] [1].

[1,2] Sánchez D & Rodríguez M. Federman, Seguridad Nacional: El realismo y sus contradicciones, Desafíos 2006. Universidad del Rosario

"La historia de los sistemas de Interceptación como Echelon es tan antigua como la propia radio. El primer escándalo internacional sobre escuchas subrepticias estalló en 1920, cuando el Senado estadounidense descubrió que unos agentes británicos copiaban todo telegrama internacional despachado por las empresas telegráficas de Estados Unidos. Las redes internacionales actuales se tendieron en las etapas iniciales de la Guerra Fría, cuando muchas naciones occidentales empezaron a vigilar conjuntamente a la Unión Soviética"[2] [1].

1.1.1. Generalidades

1.1.1.1. Seguridad nacional

"La seguridad Nacional es la creación y mantenimiento por parte del Estado de una situación en la cual los fines esenciales que ordena la Constitución se puedan alcanzar sin interferencias ni amenazas. El logro de esta situación depende del empleo armónico de todas las estrategias políticas, sociales económicas y militares que de manera integral coadyuven al logro de la convivencia y el bien común". [3]

1.1.1.2. . Interceptación de comunicaciones

El código de procedimiento Penal en el Capítulo séptimo. "De la violación a la intimidad, reserva la interceptación de comunicaciones".[4] Define en qué casos la interceptación es calificada como "delito".

1.1.1.3. Delito informático y de ciberdelito

La UIT plantea la definición de este concepto así:

"Las vulnerabilidades y el insuficiente control de las tecnologías digitales les confieren un cierto nivel de inseguridad. De este estado de inseguridad se aprovechan sobre todo los delincuentes. Por otra parte, cada tecnología introduce potencialidades delictivas y ofrece oportunidades para cometer infracciones. Internet no es excepción a esta regla y el mundo de la delincuencia ha invadido el ciberespacio".

La OCDE en 1983 la definió en términos de la infracción informática como todo comportamiento ilegal, inmoral o no autorizado que afecta a la transmisión o al procesamiento automático de datos.

---

[2] http://www.unesco.org/courier/2001_03

[4] Código de Procedimiento Penal Colombiano

“Un delito informático (computer-related crime) es aquél cuyo objeto o medio de realizarlo es un sistema informático, está relacionado con las tecnologías digitales y se integra en los propios de la delincuencia de cuello blanco. El ciberdelito (cybercrime) es una forma del delito informático que recurre a las tecnologías de Internet para su comisión, refiriéndose por tanto a todos los delitos cometidos en el ciberespacio.

El mundo virtual confiere al delito la capacidad de automatización, permitiendo su ejecución a gran escala (ciberepidemia), su comisión a distancia a través de las redes (ubicuidad del delincuente en el tiempo y en el espacio) y, en su caso, con efecto retardado (Figura 1).

Figura 1-1: Características del delito informático [2]

1.1.1.4. Infraestructura de telecomunicaciones y autopistas de la información

Se denomina infraestructura de telecomunicaciones al conjunto de medios de transmisión a partir de los cuales pueden desarrollarse servicios de comunicaciones. Efectivamente, se disocian las vías y las técnicas de encaminamiento de las soluciones y servicios de telecomunicaciones ofrecidos a los clientes. Así por ejemplo, resulta posible explotar una infraestructura existente sin ser propietario de la misma y ofrecer, a partir de ésta, facilidades de transporte para aplicaciones particulares.

La disponibilidad de equipos multimedios, de infraestructuras de comunicación eficaces, así como la convergencia de los mundos audiovisual, informático y de las telecomunicaciones, contribuyen a realizar el concepto de cadena de información totalmente digitalizada. Esto representa la continuidad digital existente, tanto a nivel de la

infraestructura de transporte como al del contenido, entre todas las fuentes de información y sus usuarios.

El concepto de autopista de la información integra la puesta a disposición del público en general; de infraestructuras de comunicación eficaces, de un conjunto de servicios de interés general o de servicios comerciales que se supone contribuyen al bienestar de los individuos y pueden estar relacionados con la sanidad, la educación, la cultura, la ordenación del territorio, la administración o la prensa, entre otros. Debido a la naturaleza de ciertos servicios ofrecidos por Internet, este medio de comunicación puede considerarse una autopista de la información.

1.1.2. Situación de la interceptación telefónica en Colombia

Colombia vive hoy una serie de hechos relevantes que afectan directamente sus estamentos, el tema de estudio es uno de los que ha llevado al Gobierno Nacional a tomar decisiones como la sustitución de funcionarios de cargos muy importantes como la Dirección de Inteligencia de la Policía Nacional DIPOL, hasta la transformación del Departamento Administrativo de Seguridad (DAS). Estos hechos consecuencia de acciones relacionadas con la interceptación de líneas telefónicas, han merecido especial atención del Gobierno y las autoridades en general concentrando la atención de muchos sectores como los económicos, políticos y gobiernos de otros países.

En Colombia la constitución Política [2], garantiza en el titulo 1 la inviolabilidad de la privacidad y el derecho a la comunicación", al mismo tiempo determina que se debe garantizar la vida honra y bienes de todo residente en Colombia". Entonces se abre el planteamiento del "bien Común" Vs "Bien Individual", Cuales quiera que sea el resultado de este debate, el Estado debe garantizarlos sin lugar a distinción, y para ello está en la potestad de emplear todas las herramientas que coadyuven a la Seguridad Nacional, como se enuncio en su significado, es aquí donde las tecnologías de la Información y las Comunicaciones tienen alto impacto dado su desarrollo y alcance, estas pueden usarse para contribuir al desarrollo social, político y económico de los pueblos, pero a su vez también para causar daño a las personas y sociedades en general.

La carta magna de nuestro País [2], también establece las obligaciones que tiene el Estado con cada uno de sus habitantes. "…servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar…, defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo[5].

[5] Constitución Política de Colombia del 2001, Titulo 1; De los Principios fundamentales, articulo 2. Título II; de los derechos, las Garantías y los deberes, articulo 15.

En cumplimiento de los principios de Bienestar de la sociedad, los Estados necesitan disponer de herramientas regulatorias que les permitan estar fortalecidos en todas las áreas en que se desarrolla la sociedad, así por ejemplo en el área de las comunicaciones; esenciales en toda sociedad, el sector de las telecomunicaciones contribuye cada día con nuevos desarrollos tecnológicos que dinamizan el proceso de la comunicación, los cuales están a disposición de los individuos quienes los utilizan conforme a sus necesidades, empero, algunas personas u organizaciones emplean la tecnología con fines ilegales, actividades que han ocasionado una gran preocupación de las autoridades que regulan a nivel internacional el sector de las telecomunicaciones como la Unión Internacional de Telecomunicaciones (UIT), entidad que se ha pronunciado oficialmente mediante el Documento denominado "Guía de ciberseguridad para los países en desarrollo Edición 2007" [2], en el cual se proponen estrategias y se recomienda a los Estados generar la regulación necesaria para contrarrestar los denominados "delitos informáticos".

El desarrollo de las TIC, ha "revolucionado" la forma de vida social, cultural, económica y política de todos los países, ha contribuido a nuevas formas de comunicación, manejo de la información, desarrollo de nuevos modelos de negocio, nuevas formas de educación etc. Sin embargo es deber de los Estados garantizar el bienestar de sus ciudadanos, reflejado en la "Seguridad del Estado".

Por lo anterior es necesario echar una mira al "nuevo planteamiento de la seguridad" en el entorno de las Tics, que da la Unión Internacional de Telecomunicaciones (UIT), la cual indica que: "La conciencia de la fragilidad del mundo digital y de la falta de control total no sólo de las tecnologías e infraestructuras informáticas y de las telecomunicaciones sino también de las soluciones de seguridad comercializadas debe plantear serias cuestiones en cuanto a la dependencia de una tecnología difícilmente controlable. El secuestro de los datos por soluciones informáticas es una realidad que no es necesario ocultar.

…Las medidas tradicionales de seguridad no podrán proteger correctamente los recursos sensibles o críticos de las personas, de las organizaciones y de los Estados, si no se realizan de modo transparente, verificable y controlable. La implementación de una estrategia completa de seguridad que integre las fases de prevención, protección, defensa y reacción pasa por la adopción de medios humanos, jurídicos, tecnológicos y económicos que permitan su realización [2].[6]

En aras de contribuir a mitigar los hechos que vulneren la Seguridad del Estado y en consecuencia el Bienestar de la Sociedad, los organismos de Seguridad del Estado adoptaron recursos humanos y tecnológicos para realizar esta función constitucional, con este propósito se adquirieron equipos de inteligencia (año 2005 se adquirió equipos de

[6] Guía de ciberseguridad para los países en desarrollo, UIT (Unión Internacional de Telecomunicaciones). 2007. Pág. 96 de 165.

interceptación y grabación telefónica), los cuales no se pudieron utilizar debido a la obsolescencia tecnológica de las redes de entonces [4],[7] por lo cual se infiere la necesidad de un estudio que permita formular estrategias para la adquisición de tecnologías de este tipo.

Por otra parte se requiere un análisis regulatorio, toda vez que como consecuencia de las interceptaciones se han involucrado diferentes entidades como el Departamento Administrativo de Seguridad (DAS); (liquidado en el año 2011 y en su lugar creo la Agencia Nacional de Inteligencia), la Fiscalía General de la Nación, la Policía Nacional a través de la Dirección de Inteligencia y Policía Judicial (DIJIN) y sus unidades descentralizadas (Seccionales de Inteligencia y Policía Judicial: SIJINES).

La "Seguridad del Estado", conlleva a la necesidad de plantearse unas estrategias técnicas que permitan una incorporación adecuada de las Tecnologías de la Información y las Comunicaciones (Tics) y un análisis regulatorio que la impulse conservando los derechos ciudadanos de privacidad y libre expresión.

Con este trabajo se pretende realizar aportes en diferentes ámbitos relacionados con las telecomunicaciones tales como: a) la optimización de recursos que hace referencia a un mejor aprovechamiento de los medios tecnológicos y humanos con los que cuenta el Estado y b) fortalecimiento de la regulación de Telecomunicaciones que se relaciona con los procesos de interceptación telefónica.

Respecto de la optimización de recursos, se espera a través del desarrollo de la investigación proponer la creación de un marco regulatorio legal para que las interceptaciones que buscan fortalecer la seguridad de la Nación no sean consideradas delitos. También se pretende que por medio del análisis técnico se logre optimizar el uso de los recursos Humanos y tecnológicos del Estado.

En los último años se vienen presentando en Colombia una serie de hechos delincuenciales donde cada vez el uso de las Tics con ese fin tiene mayor auge, los delitos se ejecutan desde llamadas extorsivas hasta acciones financieras donde "expertos", vulneran las bases de datos de los bancos y extraen información privada para ejecutar sus fines ilegales. [8]

Por otra parte las Transnacionales del sector de las comunicaciones han dejado toda la carga al Estado respecto de la implementación de las tecnologías para tener acceso a sus redes y realizar los procedimientos de interceptación legales, sopena de pérdida de

[7] Informe de la Contraloría de Bogotá, No. 35000- **3462** 30 de enero de 2006, Ref. Control de advertencia sobre "deficiencias en la instalación y funcionamiento de equipos destinados al fortalecimiento de la Seguridad Ciudadana en Bogotá, D.C."

[8] Fuente: Alertan sobre llamadas extorsivas, Periódico el País: Octubre 16 de 2009. Disponible en http://www.elpais.com.co/historico/oct162009/JUD/extorsion.html

recursos cuando se adquieren tecnologías no compatibles con las que tienen los operadores telefónicos, situación que amerita un análisis y el estudio de las condiciones que se tienen en otros países (citados anteriormente) por parte de los Estados sobre los operadores telefónicos.

Finalmente es importante considerar que el Estado debe estar preparado para garantizar los derechos de los ciudadanos consagrados en la Constitución, mediante la incorporación de las herramientas necesarias para cumplir el mandato constitucional, de la misma forma debe dinamizar la legislación a fin de que esta no esté distante para ejercer un control eficiente y contrarrestar el desarrollo de nuevas formas delictivas que evolucionen a la par con el desarrollo de nuevas tecnologías por ejemplo las redes de Nueva Generación (NGN).

Como se ha registrado en el Marco Teórico, el uso de las Tics, es una preocupación de países Desarrollados y en vía de Desarrollo, pues este sector requiere ser regulado por los estados, y orientar su principal potencial al bienestar de la humanidad.

Para ejercer el control de las Tics, se empelan métodos para el control de la información que circula a través de ellas, uno de ellos es la "Interceptación telefónica", este tema implica dos puntos de análisis y estudio: Por un lado la regulación que involucra a los operadores de servicios de telefonía, las autoridades que realizan estos procedimiento y por otro lado los procedimientos de implementación y adquisición de estas tecnologías.

En los puntos de vista tratados, conforme al recorrido por la normatividad Nacional e internacional, se demuestra que los países citados como: Estados Unidos, Canadá, Gran Bretaña, México, España, Ecuador y Colombia, han trabajado normas resientes orientadas al tema de la Interceptación. El caso que ha impulsado y de alguna forma pretende justificar la interceptación fueron los hechos del 11 de septiembre de 2001. En esta materia se dan opiniones a favor y encontrar de la interceptación, algunos hechos positivos tratan de soportarla, un ejemplo de esto es que "en los últimos años esta herramienta ha sido de suma importancia en la lucha contra el terrorismo, el crimen organizado y, en general, la delincuencia sofisticada. Muestra de ello es el reciente rescate de Ingrid Betancourt y los otros 14 secuestrados, una jugada maestra de las fuerzas militares, donde éste fue un instrumento clave"[9] [5].

Queda demostrado que esta herramienta es vital para diversos fines, siempre y cuando garanticen el bienestar de la sociedad. Aquí surge una inquietud, es factible fortalecer el uso de estas herramientas y orientarlas al beneficio de los estados?, dada su relación intrínseca con las tecnologías pues son estas las que la hacen posible, es imprescindible hacer el estudio de su aplicación a través del desarrollo de las tecnologías, en consecuencia hoy la normatividad no puede considerar la interceptación en los términos

[9] *Asociación de Profesores de Derecho Penal, Articulo: "Legalidad de la interceptación de comunicaciones en Colombia", consultada el 20 de octubre de 2009, disponible en www.larepublica,com.co.

de líneas telefónicas fiscas; vistas como pares de cobre o abonados celulares con frecuencias definidas que son posibles de escuchar o desencriptar mediante equipos especiales. La convergencia y la modernización de las redes hoy hacen que no se distinga entre un canal de voz y uno de data, “son lo mismo”, y como hemos visto en el estudio de la normatividad esta no está legislada en torno a los nuevos desarrollos.

Otro factor importante de analizar es que los nuevos operadores de comunicaciones, ya no son fijos y pertenecen y actúan en un único país, estos hoy son multinacionales que prestan sus servicios desde diferentes países, a su vez ya han aparecido los operadores móviles virtuales, haciendo todos usos de las redes de Nueva generación (NGN), y si bien es cierto la regulación se ha quedado corta Vs desarrollo tecnológico, también es importante analizar, porque Colombia ha entregado su mercado a estas empresas y además debe asumir los costos para ejercer el control de la información que transite a través de las redes de estos operadores?, acaso no hay forma de trasladar los costos que ha tenido que asumir el País como son “la infraestructura del proyectos Esperanza” por ejemplo a estos operadores, no se trata de indicar que ellos entreguen al estado el dinero que se invirtió en esa tecnología, sino que los futuros costos para que el estado disponga de estas tecnologías de control y acceso a las redes sean asumidas por los operadores de estos servicios.

Esta alternativa fundamenta el hecho que Colombia ha sacrificado el desarrollo e inversión en otros sectores sociales, apartando grandes recursos para la compra de equipos para la interceptación, los cuales al momento de ponerlos en operación han presentado obsolescencia tecnológica, ocasionándose inmensas pérdidas económicas, además de los problemas disciplinarios para los funcionarios que estuvieron a cargo de los procesos de Gestión tecnológica.

Es entonces muy importante revisar los modelos de Gestión de tecnología de países desarrollados y plantear alternativas dinámicas para que tanto las normas como las tecnologías no se queden rezagadas ante los desarrollos de la Tics y que el Estado (la sociedad) asuma estos costos.

1.1.3. Función de las instituciones Públicas.

Las instituciones públicas necesitan más que nunca desempeñar su función tradicional de persecución y represión de los fraudes y delitos. Asimismo deben ser activas en materia de sensibilización y de información de la población. Sería extremadamente útil poder disponer de elementos de referencia relativos a la protección de las personas y bienes cuando se utiliza Internet.

Cada vez será más peligroso permitir que las fuerzas de orden queden retrasadas en el dominio tecnológico. Efectivamente, un eventual esfuerzo de puesta al día tras varios años no solamente tendría un coste financiero directo, consecuencia de las inversiones en nuevas infraestructuras, sino también y sobre todo un coste social por el auge de la

influencia de las estructuras mafiosas o asimiladas sobre la sociedad, con todos los riesgos de desestabilización que ello comporta [2].

Sin embargo, el crecimiento excesivo de la presencia policial en la red no es forzosamente deseable, ya que puede entrar en conflicto con la necesidad de confidencialidad de los intercambios y de respeto a la esfera privada de los individuos.

1.2. El Proceso de interceptación telefónica

El Proceso de interceptación telefónica, depende directamente de la tecnología que se desee accesar. Se conocen dos métodos, formas o modos de realizar la interceptación telefónica.

Estos modelos son: el tradicional y el actual, el primero está orientado a tecnologías análogas, la cual utiliza la cinta magnetofónica mientras el segundo utiliza los medios de almacenamiento digital como el DC, Discos duros (DD), Memorias (USB) entre otros.

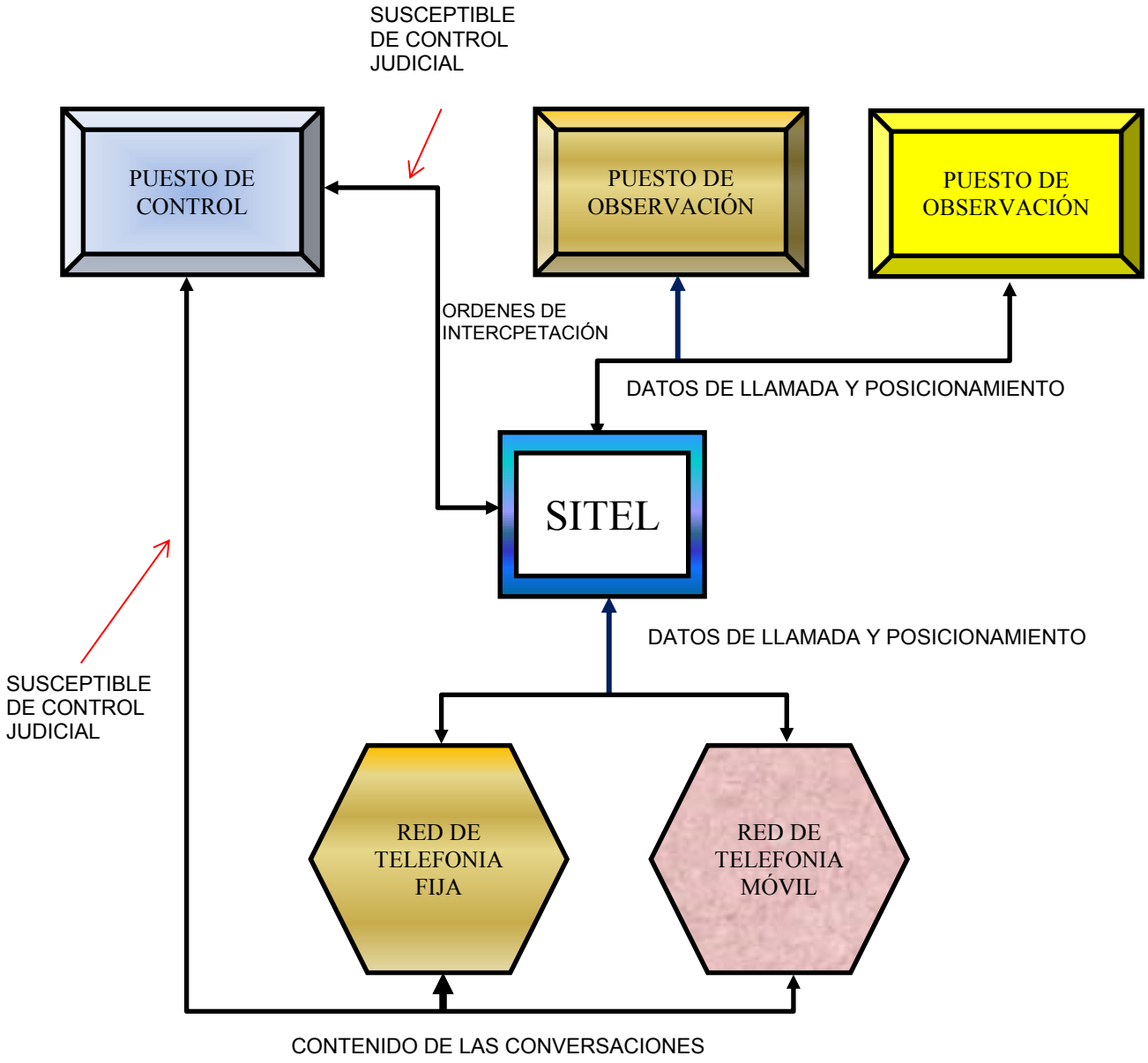
Para ilustrar el proceso de interceptación, tomemos como ejemplo el sistema SITEL, utilizado en Europa, cuyo diagrama en bloques se muestra en la figura 2-2.

“SITEL (Sistema Integrado de Interceptación Telefónica) es una estructura para realizar escuchas telefónicas que incluyen dos centros de monitorización, salas de monitorización y terminales remotos distribuidos. Centraliza la información recibida de las facilidades de interceptación que las operadoras de telefonía (TME, Amena, Vodafone y Telefónica de España) han incorporado a sus redes”[11].

En la práctica el 'software espía' forma parte de los programas que hacen funcionar las redes; cuando es activado, este software envía copia de toda la información relevante a las salas y centros de monitorización a través de las terminales remotas. En estos centros la información es controlada, seleccionada y enviada al juzgado correspondiente, al parecer mediante DVDs grabados [2] [11].

En la figura 2-3, se presenta un paralelo entre los procedimientos de interceptación; el antes o tradicional, procedimiento manual en el cual una persona debe accesar la línea objetivo en forma física, y el después, un proceso con nueva tecnología, mediante la configuración de la plataforma SITEL.

Figura 1-2: Sistema Integrado de Interceptación Telefónica (SITEL)[10]

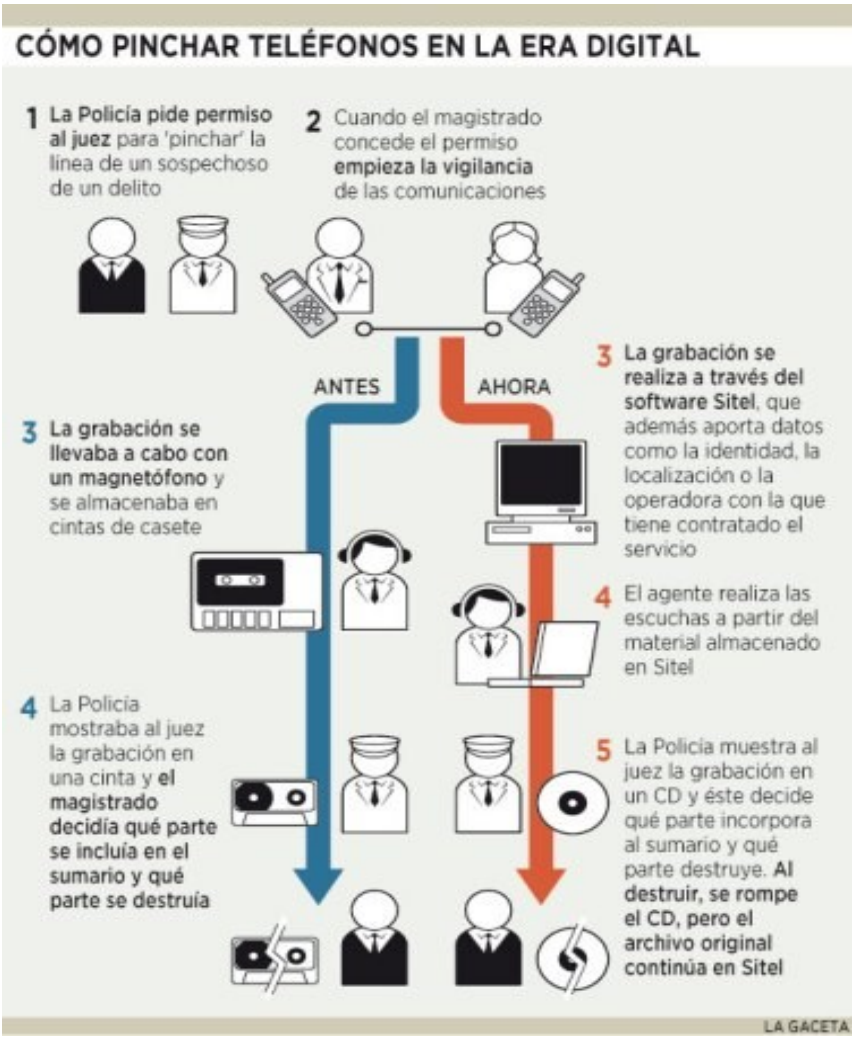


Este sistema es usado "para interceptar y analizar cualquier tipo de comunicaciones digitales (llamadas telefónicas de fijos y móviles, mensajes de texto e imagen, localización geográfica en el caso de móviles, etc.). No consta, pero es probable, que el

[10] Fuente: http://www.spanishred.com/foro/

sistema tenga capacidad de interceptar comunicaciones de Internet como correo electrónico y navegación web (al estilo del estadounidense Carnívora).Carnívora es el nombre de un software usado por el FBI.

Figura 1-3: Paralelo entre las dos tecnologías [6]



Este software se instala en los proveedores de acceso a Internet y, tras una petición proveniente de una instancia judicial, rastrea todo lo que un usuario hace durante su conexión a Internet.

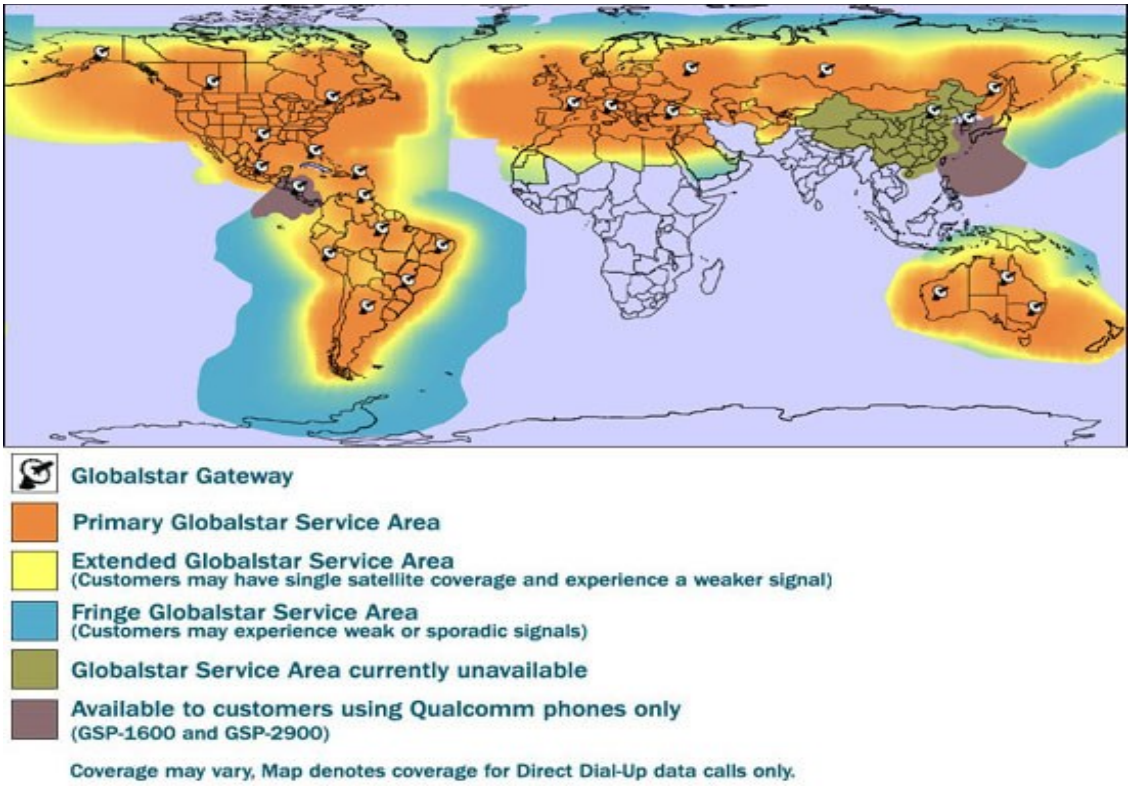
En teoría tiene capacidad para discernir comunicaciones legales de ilegales. El cómo realiza este análisis, y cuál es su infraestructura y alcance real, es algo que permanece

secreto. Tiene la misma procedencia que ECHELON (EE. UU.) y pertenece a una agencia estatal (FBI), al igual que ECHELON (NSA)[11]

Otros sistema de interceptación y quizás el más importante y sofisticado del planeta es "ECHELON" "Red global de interceptación de comunicaciones controlada por la Agencia Nacional de Seguridad estadounidense".

La figura 2-4, presenta la red del sistemas de comunicaciones satelital que a nivel mundial, opera para el sistema echelon.

Figura 1-4: Cubrimiento de sistemas de comunicaciones Globalstar Gateway



"Echelon arranca en 1947, tras la Segunda Guerra Mundial, y su finalidad era originalmente espiar a los soviéticos. Pero con el tiempo derivó en el espionaje industrial y de eso a la información económica y política en Europa. El proyecto inicial contaba con la participación del Reino Unido, Australia y Nueva Zelanda"[12].

Esta red de espionaje de Estados Unidos, Canadá, Australia y Nueva Zelanda capta todos los mensajes que dejan un "rastro electrónico", los selecciona y los almacena al

[11] http://www.spanishred.com/foro/
[12] Fuente: http://ecodiario.eleconomista.es/telecomunicaciones-tecnologia/noticias

servicio de los intereses de sus gobiernos o empresas. Teóricamente tiene capacidad para interceptar tres millones de comunicaciones por minuto.

Este sofisticado sistema de interceptación, nacido al finalizar la Segunda Guerra Mundial y que continúa plenamente operativo, se ha utilizado con fines militares, pero también económicos e incluso privados.

Echelon es un reducido y brillante equipo de estadísticos, lingüistas y matemáticos que trabajan en un lugar secreto, rastrean y analizan todas las comunicaciones internacionales por voz, fax y email. Este equipo ha servido a EEUU durante años para detectar indicios de criminalidad contra sus intereses y localizar a presuntos terroristas, creando alertas de riesgo y algoritmos de criminalidad.

Cuenta con datos recogidos por 120 satélites espía y su capacidad técnica incluye la interceptación de todo tipo de mensajes transmitidos por vía satélite. Al elaborar el informe de la Eurocámara, sus autores recogieron testimonios de compañías europeas que denunciaban haber sido espiadas.

El caso más conocido fue el de Airbus, que aseguró haber perdido un contrato de 6.000 millones de dólares con el Gobierno saudí, que optó por la compañía estadounidense Boeing y McDonnell Douglas gracias a información desde Echelon.[13]

1.3. Sistemas de interceptación a nivel mundial

1.3.1. Sistema Echelon

Es la Agencia Nacional de Seguridad de los Estados Unidos, es quien realiza la administración principal del sistema, esto significa que es quien tiene prioridad en el conocimiento y manejo de la información. La figura 2-5 presenta su escudo, que la identifica como la agencia más poderosa a nivel mundial en manejo de información secreta, por lo tanto estratégica y sensible, en lo político, comercial y militar.

[13] Fuente: Tomado de http://ecodiario.eleconomista.es/telecomunicaciones-tecnologia/noticias/

Figura 1-5: Escudo de la Agencia Nacional de Seguridad de los Estados Unidos

"En los lugares más remotos del planeta proliferan unas semiesferas blancas de 30 a 50 metros de diámetro. Como constelaciones de gigantescas pelotas de golf, brotan en los arrozales del norte de Japón y en los viñedos de la Isla del Sur de Nueva Zelandia. La figura 2-6 consiste en una de las estaciones de este sistema.

Figura 1-6: Base de escucha en Menwith Hill, Reino Unido[14]

[14] Ibídem

Echelon Constituyen la señal más ostensible de las redes electrónicas ocultas que vigilan el mundo. Cada semiesfera está repleta de antenas de seguimiento por satélite que absorben y examinan silenciosamente millones de faxes, llamadas telefónicas, mensajes de correo electrónico y datos informatizados. Sin que los emisores lo sepan, estos mensajes pasan de los montículos a redes informáticas y a auditores que pueden encontrarse en el otro confín del mundo.

Como éste se ha globalizado y las comunicaciones son decisivas para la actividad humana, esas redes de escucha han aumentado de manera exponencial. Forman parte de los llamados sistemas de captación de señales o sigint, manejados por un puñado de países avanzados. En la siguiente figura se pueden ver la distribución de sistemas de recepción de la red.

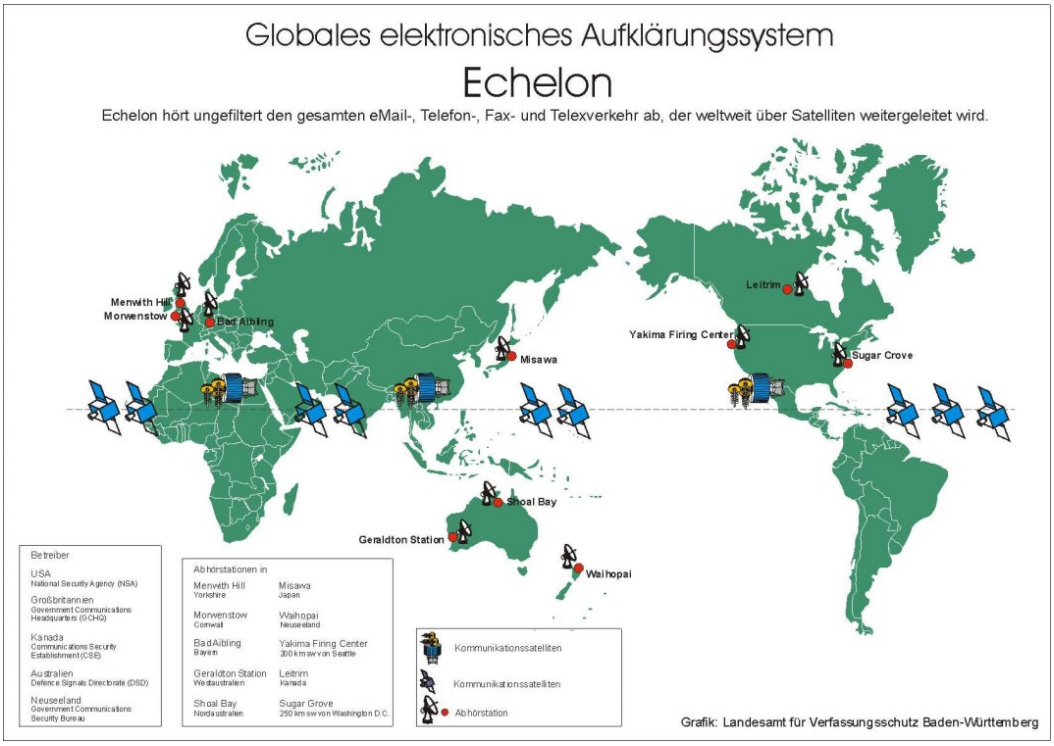
Figura 1-7: Localización de los puntos de escucha de la Red Echelon.[15]

Durante muchos años, la existencia de las redes de sigint permaneció en secreto: en los países interesados la ley desaconsejaba e incluso prohibía toda alusión a ellas. Actualmente, el Parlamento Europeo está realizando una cuidadosa investigación sobre las organizaciones de sigint y cómo pueden vulnerar los derechos humanos o interferir en el comercio internacional. La preocupación europea se centra en Echelon, un sistema que conecta las estaciones de escucha de diez países a fin de interceptar y procesar las comunicaciones internacionales por satélite. Echelon es sólo un eslabón de una inmensa

[15] Fuente: tomado de: http://www.unesco.org/courier/2001_03

red controlada por Estados Unidos y sus aliados de habla inglesa como el Reino Unido, Canadá, Australia y Nueva Zelandia; denominada UKUSA en virtud de un acuerdo secreto que constituyó dicha alianza en 1948. Es muy poco lo que se sustrae al control de UKUSA, que intercepta mensajes transmitidos por Internet, cables submarinos y radioemisoras, así como los procedentes de los equipos de vigilancia instalados en las embajadas. El sistema funciona incluso en el espacio, por medio de una flota de satélites orbitales como se puede ver en la figura 1-8.

Figura 1-8: Localización de los puntos de escucha de la Red Echelon. [7]



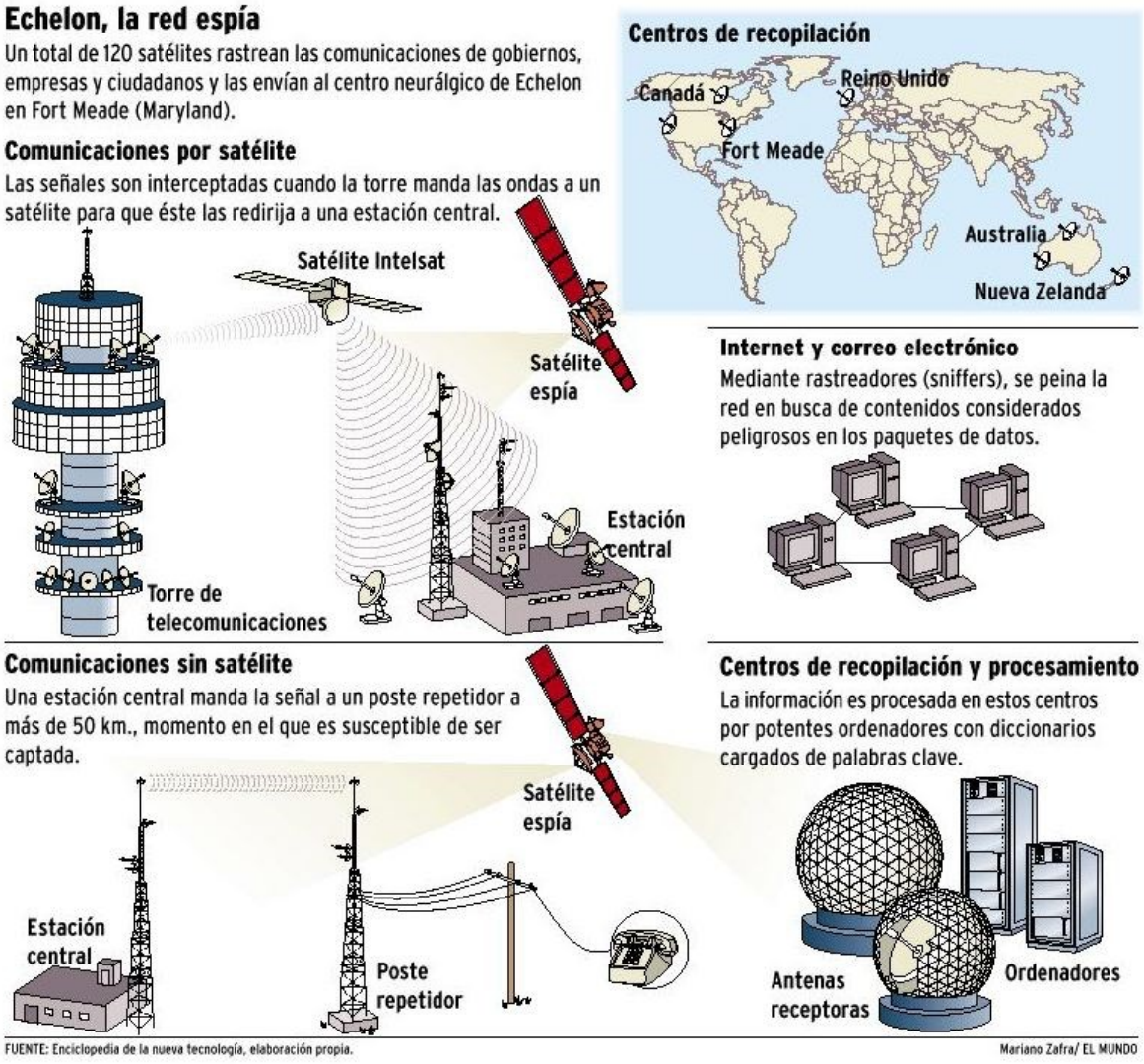
1.3.1.1. Funcionamiento de la red Echelon

La figura 2-9, presenta en forma general el funcionamiento de Echelon, en cuanto a su forma de transporte de la información desde los diferentes puntos de recepción, terrestres y satelitales.

La cuestión esencial radica en el funcionamiento de este sistema. Una vez definidos los objetivos del espionaje, resulta evidente el carácter titánico de la tarea encomendada a ECHELON: vigilar “todas” las comunicaciones que se realizan en el mundo. A primera vista, tal tarea parecería imposible y hasta absurda. Primero por la complejidad y las dificultades tecnológicas que implica el diseño de un sistema capaz de interceptar los millones de millones de comunicaciones que se realizan diariamente en el mundo. Segundo, y sobre todo, por las cantidades de información generada, cuyo tratamiento y

análisis escaparía a los acelerados tiempos del espionaje. Lo interesante del caso ECHELON es que las tecnologías utilizadas ofrecen la posibilidad de alcanzar "lo esencial" de tan descomunal tarea.

Figura 1-9: Operación de la de la Red Echelon. [16]



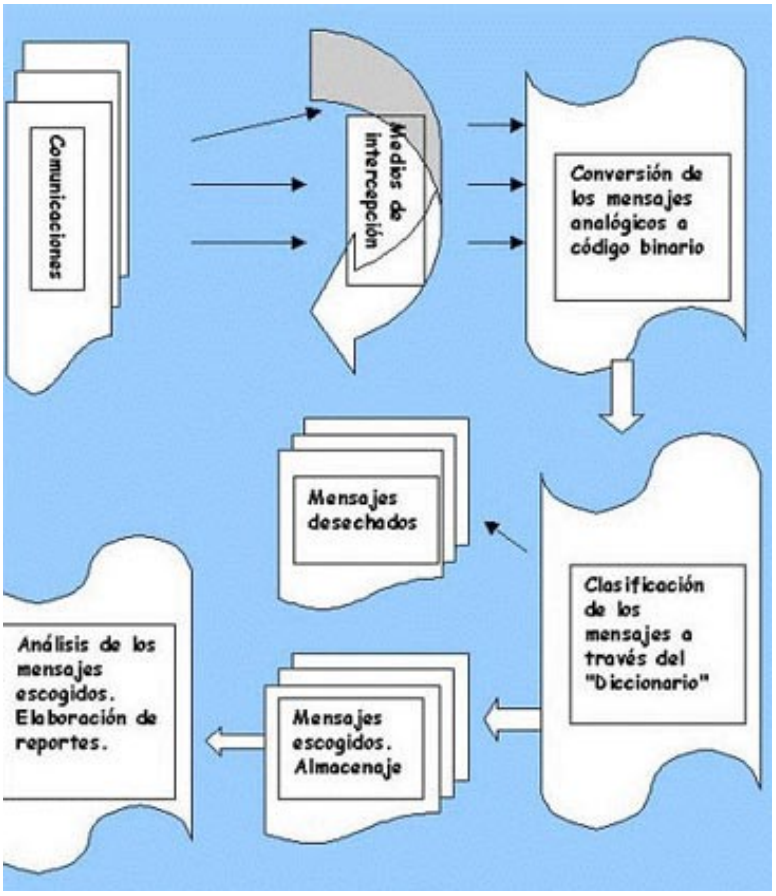
En cuanto al manejo, procesamiento y análisis de la información, la figura 2-9, presenta un diagrama en bloques de los grandes procesos, que tienen lugar en la estructura de Echelon.

La primera capa de ECHELON consiste en los medios de interceptación que captan las comunicaciones y las transmiten a los centros de tratamiento, ello comprende: las

[16] Fuente: http://extrados.mforos.com/606888/2662145-echelon-red-mundial-de-espionaje-electronico/

estaciones terrestres, los medios navales espías y los satélites secretos ubicados a gran altura (mayor que la de los satélites civiles). El espionaje en Internet se realiza a través de los servidores raíz, la mayoría de las cuales está manejada por empresas o instituciones estadounidenses.

Figura 1-10: Proceso de la información en el sistema Echelon. [17]



Los estudiosos de ECHELON ubican 11 importantes estaciones terrestres de espionaje, cuyo objetivo principal son las transmisiones de los sistemas satelitales, en particular los sistemas Intelsat e Inmarsat. Otras estaciones terrestres, que operan por lo general en bases militares, se encargan de rastrear las transmisiones radiales de alta frecuencia, ligadas con comunicaciones militares. La red de satélites espías se controla totalmente por los servicios estadounidenses. Está dedicada a interceptar las comunicaciones por microondas, telefonía celular, señales electrónicas y radiales. Se estima que esta red posee al menos veinte satélites participando en las tareas de espionaje.

[17] Fuente: http://extrados.mforos.com/606888/2662145-echelon-red-mundial-de-espionaje-electronico/

El siguiente nivel de ECHELON es el primer tratamiento de la información. Una vez interceptados, los mensajes son convertidos (si conviene) en código binario, mediante tecnologías informáticas (reconocimiento de caracteres y de la voz). Tal es el caso de los sistemas de reconocimiento de la voz, capaces de convertir en texto las conversaciones telefónicas. ECHELON cuenta con un sistema llamado Voicecast, que permite establecer un patrón de voz y rastrearlo para moorear todas las llamadas de la persona bajo "observación". La intercepción da como resultado cantidades inconmensurables de información. La solución aplicada por el sistema es el establecimiento de principios para discriminar las "escuchas" útiles de las desechables. Ello se concreta en aplicaciones informáticas capaces de analizar los documentos buscando ciertos patrones (palabras, nombres, sitios, códigos, números de teléfono y otros).

Los llamados "Diccionarios" o compendios de "palabras clave" constituyen la base de tales programas. En ellos, los diferentes servicios de espionaje incluyen los criterios que deben ser rastreados en los mensajes interceptados. Y así, la cantidad de información por analizar se reduce drásticamente. Solo los mensajes que contienen un término incluido en el "Diccionario" son grabados y, en ciertos casos, analizados. Hasta ese momento, todo el proceso es automatizado: la intercepción, la codificación, la búsqueda a partir de los diccionarios se realiza con dispositivos automáticos, entre los cuales destacan las computadoras de procesamiento masivo. Con los mensajes "escogidos", los analistas de ECHELON elaboran diferentes tipos de informes: traducción y compilación de las intercepciones, clasificaciones por temas, por personas y otros, según las necesidades del "cliente". Este procedimiento se denomina "Control estratégico de las telecomunicaciones".

He aquí una muestra fehaciente del pensamiento de las clases dirigentes de los EE.UU. quienes manejan los hilos de ECHELON, “Para que la globalización funcione, EE.UU. debe actuar sin miedo como la todopoderosa superpotencia que es. La mano oculta del mercado nunca funciona sin la ayuda de un puño oculto. McDonnald´s no podría florecer sin McDonnel Douglas, el proyectista de los aviones de combate F-15; y el puño oculto que garantiza la seguridad de un mundo en el que puede prosperar la tecnología del Silicon Valley se llama Ejército, Fuerza Aérea, Armada y Cuerpo de Marines de los EE.UU.”. Thomas Friedman. The New York Times. 20 de marzo de 1999.

ECHELON suministró a las autoridades de los EE.UU. una alerta de tres meses antes de que se realizaran los ataques contra las Torres Gemelas. Un artículo aparecido en el diario Frankfurter Allgemeine Zeitung, de Alemania daba cuenta de que los servicios de inteligencia israelí y estadounidense recibieron señales de aviso al menos tres meses antes de que se realizaran los secuestros de los aviones comerciales y su conversión en armas para atacar símbolos del imperio norteamericano

Pese al extraordinario alcance de Echelon y de los sistemas equivalentes, es falso que pudieran interceptar “la totalidad de las comunicaciones por correo electrónico, teléfono y fax”. Tampoco son capaces de reconocer el contenido de todas las comunicaciones telefónicas. Y es pura fantasía que el mero hecho de que dactilografiar una palabra clave

como “bomba” en un e-mail ponga en marcha una grabadora de cinta magnética en alguna base secreta. De cada millón de comunicaciones telefónicas o mensajes que se intercepten, menos de diez servirán para obtener información. Y la mayoría de las comunicaciones personales se ignoran, salvo las de personas “importantes”, como políticos, hombres de negocios de primer plano, y sus familias.

En todo el mundo abundan las acusaciones y sospechas de escuchas telefónicas sin control judicial, en especial por parte de los servicios secretos. En Francia ha habido varios casos de escuchas con finalidades políticas, por ejemplo durante la presidencia Miterrand. En el Reino Unido se grabaron conversaciones íntimas del heredero de la corona, e incluso periódicos han llevado a cabo escuchas ilegales.

En los EE UU se sospecha que entidades como la National Security Agency han usado sistemas de escuchas ilegales adjuntos a las mismas redes telefónicas, del estilo de la Habitación 641A, una instalación situada en un edificio de la telefónica SBC en San Francisco.

En Grecia, durante las Olimpiadas de 2004 y después, más de 100 teléfonos móviles pertenecientes a autoridades (incluyendo el Primer Ministro de la época, Kostas Karamanlis) fueron espiados mediante un sistema informático no autorizado instalado en la red de la telefónica Vodafone. Jamás se llegó a averiguar quién estaba detrás, aunque se sospechó de servicios secretos extranjeros, y Vodafone Grecia fue multada.

2. Estudio de la regulación Nacional e Internacional en materia de interceptación telefónica.

Un estudio objetivo de la normatividad y/o regulación de la interceptación telefónica debe considerar en el caso colombiano, la fuerza normativa de algunas disposiciones de derecho internacional que Colombia ha aceptado e incluido en el bloque de constitucionalidad, a través de tratados internacionales y que encuentra su fundamento en la Constitución Política. El articulo 93; que trata sobre tratados y normas de derechos humanos[18] [8]. Esto indica que Colombia no está regida solamente por la constitución, sino también las que se derivan de tratados internacionales de derechos humanos[19] [9]. Por eso se deben cumplir y acatar normas de organismos internacionales como: Comisión Interamericana de Derechos Humanos (CIDH), Corte Interamericana de Derechos Humanos (CIDHH) y Órganos de derechos humanos de la Naciones Unidas.

2.1. Organismos y normas internacionales

2.1.1. Convención Americana sobre derechos humanos.

El Articulo 11.2 de esta convención establece que “Nadie puede ser objeto de injerencia arbitraria o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación” “...puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo,

[18] Jaime Rodríguez v. Iván Mejía Álvarez, sentencia T-1319, Corte Constitucional, 7 de diciembre de 2001, disponible en:
<http://www.corteconstitucional.gov.co/relatoria/2001/t-1319-01.htm>
[19] Rodrigo Uprimny Yepes, Bloque de constitucionalidad, derechos humanos y nuevo procedimiento penal, Escuela Judicial Lara Bonilla, Consejo Superior de la Judicatura, Bogotá, 2006.

el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones" [20] [10].

2.1.2. Pacto Internacional de Derechos Civiles y Políticos

En su artículo 17 establece: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación".

- Los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones:

Entre otras indicaciones, establece que la Vigilancia de comunicaciones solo puede darse con orden de autoridad legítima, para lo cual debe ser proporcional y para esto debe ser:

a) Cumplir un fin legítimo
b) Ser idónea para alcanzar ese fin
c) Ser necesaria
d) Ser proporcional en estricto sentido

2.1.3. Caso España

2.1.3.1. Concepto de interceptación telefónica

"Aquellas medidas instrumentales restrictivas del Derecho fundamental del secreto de las comunicaciones privadas, ordenadas y ejecutadas en la fase instructora de un proceso penal bajo la autoridad del órgano jurisdiccional competente frente a un imputado, u otros sujetos que de este se sirva para comunicarse,….investigar determinados delitos, descubrir al delincuente y en su caso aportar al juicio oral determinados elementos probatorios (...actos de investigación sumarial) [11]" [21].

[20] Corte Interamericana de Derechos Humanos, sentencia de 6 de julio de 2009, Serie C No. 200, párr. 114.
[21] Montoya, Mario Daniel; Informantes y técnicas de investigación encubiertas, 2da Ed. AdHoc Buenos Aires. Pág. 368.

La intervención telefónica puede ser interpretada en el sentido que cuando se interceptan comunicaciones, esta no se hace a la intimidad de la persona sino sobre el medio que se utiliza para cometer actos delictuosos, así el estado tiene el derecho de intervenir el medio cuando sea utilizado con fines ilegales, toda vez que "adquiere la condición de instrumento del delito"[22]

…El código procesal Militar en su art. 188 dispone que los jueces militares podrán acordar la intervención y grabación de las comunicaciones telefónicas o radiofónicas de cualquier persona cuando hubiese indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia objeto del proceso"[23].

También se establece los aspectos por los cuales estaría limitada la interceptación Telefónica:

a) Por el delito
b) Por el tiempo
c) Por el espacio
d) Por las personas
e) Por el procedimiento
f) Por el medio de ejecución:

"Es necesaria una regulación que contemple el sistema técnico que va a ser empleado para la interceptación telefónica y para la grabación de la conversación"[24].
Como normas internacionales en España sobre Interceptación Telefónica se encuentran:

- La declaración Universal de los Derechos Humanos
- El Pacto Internacional de Derechos Civiles y Políticos

"En la sentencia del 6 de septiembre de 1978, caso "Klass", y otros, el Tribunal Europeo de derechos Humanos afirmó que las sociedades democráticas se encontraban amenazadas por formas complejas de espionaje y terrorismo, por lo que el estado para combatir eficazmente estas amenazas, debería estar capacitado para vigilar en secreto a los elementos subversivos que operaban en el territorio".[25]

En el caso Colombiano; cualquier parecido con la realidad puede tornar a fantasía, como se señaló en el Marco Teórico, la interceptación Telefónica, no es ajena a los demás países, en otrora fue herramienta justificada en pro de evitar delitos contra los estados.

2.1.3.2. Requisitos exigidos para ser válida una intervención telefónica.

[22] Ibídem. 22 pág. 369 de 671.
[23] Ibídem. 23 pág. 371 .
[24] Ibídem. Pág. 373.
[25] Ibídem. Pág. 374

…"Gran parte de los preparativos, contactos negociaciones y citas, se llevan a cabo a través de negociaciones telefónicas, de lo que se deriva que la observación de tales comunicaciones es uno de los medios de investigación idóneo cuando no el más adecuado o, el único posible para la determinación de las responsabilidades de los jefes y miembros más destacados de la organización criminal."[26]

- **Sistema de normas que regulan la interceptación en España:**

a) Artículos: 9.3, 10.1, 2* 14, 18...3, 21.1, 2*, 55.2 y 96.1 de la Convención.
b) Convenio Europeo para la Protección de los Derechos del Hombre y las Libertades fundamentales, del 4/11/50, art. 8*, ratificado el 26/9/79.
c) Declaración Universal de los derechos humanos del 10/12/48. Art 12.
d) Pacto internacional de derechos civiles y Políticos de Nueva York del 16/12/66.
e) Artículo 579 de la Ley de Enjuiciamiento Criminal.
f) Artículos 11.1, 238 y 240 de la ley orgánica del Poder Judicial.
g) El artículo 6.3 del Código Civil.
h) Jurisprudencia del Tribunal de Derechos Humanos, del Tribunal Constitucional y de la Sala Penal del Tribunal Superior.

- **Vulneraciones que Determinan la nulidad de la Prueba.**

a) No exteriorización de indicios.
b) Ausencia de Control.
c) Periodicidad del control.
d) Disociación entre autorización e investigación.
e) Entrega de copias, no de originales.
f) Constatación de la Proporcionalidad.
g) Determinación de la medida y sus límites.
h) Casos relevantes de interceptación Telefónica.

Tabla 2-1: Casos relevantes de interceptación telefónica

Año	Caso	País	Descripción
1972	El escándalo del Watergate (o Watergate)	Estados Unidos	Escándalo político en los Estados Unidos que ocurrió en 1972 durante el mandato de Richard Nixon, que culminó con la imputación de algunos consejeros muy cercanos al presidente, y con su propia dimisión el 8 de agosto de 1974. (1)

[26] Ibídem Pág. 375.

Aquí es importante resaltar qué países acogen esta Directiva: Países Bajos, Austria, Estonia, Chipre, Grecia, Luxemburgo, Eslovenia, Suecia, Lituania, Letonia, República Checa, Bélgica, Polonia, Finlandia y Alemania[27] [12].

2.1.4. Acuerdos Internacionales

Es importante anotar que Colombia, a través de los años a suscrito acuerdos de cooperación internacional, en la lucha contra delitos transnacionales, de la misma forma se ha preparado en la lucha contra el crimen organizado, de esta forma los organismos de seguridad del estado, como la Policía Nacional, cuentan con grupos profesionales que realizan operaciones especiales en determinados entornos. Ahora bien, dada la inmensa clase de delitos y modus operandi de las bandas delincuenciales, los organismos de seguridad deben especializar sus grupos en áreas específicas, con el fin de atacar la comisión de delitos en cada una. Estos esfuerzos son costosos para el estado y la sociedad, sin embargo los resultados de las operaciones los justifican. Esto a nivel local; del País, pero que pasa con los delitos de tipo internacional? En aras de contrarrestarlos, los países se han debido organizar y establecer acuerdos, donde se puedan colaborar entre sí, ya se compartiendo información, entrenamiento militar, asesoría tecnológica etc.

En la Actualidad Colombia tiene acuerdos con:

a) Francia:

Acuerdo entre el gobierno de la república de Colombia y el gobierno de la república francesa relativo a la cooperación en materia de seguridad interior.

Este Acuerdo, establece entre otros aspectos los términos o normas con que se deben tratar **los datos nominativos**, que sean informados de un país al otro, en concordancia con el acuerdo entre los dos.

"La comunicación de los datos debe hacerse especificando los fines con que ellos deben utilizarse y el periodo de uso. Al final de dicho periodo, los datos deben ser destruidos. Se considera también el intercambio de información a formas de crimen transnacional tales como: terrorismo, lavado de activos, tráfico de estupefacientes, tráfico de armas, falsificación de moneda, trata de personas, tráfico de bienes culturales e ilícitos contra la propiedad intelectual e industrial, y tráfico de recursos naturales"[28].

[27] Directiva 2006/24/CE del parlamento europeo y del consejo de 15 de marzo de 2006, disponible en: https://www.boe.es/doue/2006/105/L00054-00063.pdf

[28] Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia Por Juan Camilo Rivera y Katitza Rodríguez, Mayo 2015; Comisión Colombiana de juristas.

b) Tratado del Atlántico Norte [13]

Este tratado esta dado en materia de inteligencia; y se denomina

"Acuerdo entre la Republica de Colombia y la organizaci6n del tratado del atlántico norte sobre cooperaci6n y seguridad de información, Dado en duplicado en Bruselas, el día 25 de junio de 2013, en español, inglés y francés, teniendo los tres textos Ia misma autoridad"[29].

Este acuerdo trata de las medidas que se deben garantizar para el intercambio y protección de la información que se comparta entre los estados. Aquí se establece un compromiso para salvaguardar todo tipo de información y/o material que se entreguen las partes. A la información se le debe dar un trato de reserva especial y no se puede compartir con terceros, sin la previa autorización del País que la suministro.

c) Acuerdo con la Oficina de Policía Europea

"Agreement on Operational and Strategic Co-operation between Colombia and the European Police Office"

Firmado el 17 de febrero de 2014 y oficializado desde el 25 de febrero de 2014,

El acuerdo consiste en el intercambio de todo tipo de información acerca de delitos internacionales, para combatirlos, además acerca de investigaciones sobre narcotráfico, armas de uso terrorista, inmigración, trata de personas, lavado de dinero, lavado de activos etc. De la misma forma define las normas que se deben observar por las partes para el tratamiento y clasificación de la información, así como el nivel de confidencialidad.

d) Acuerdo con Brasil

2.1.4.1. La Interceptación según la Unión Internacional de Comunicaciones

Mediante la recomendación UIT-T Y.2201 de abril de 2007, que trata sobre las redes de la próxima generación – Aspectos relativos a los servicios: capacidades y arquitectura de servicios y establece los "Requisitos de las redes de la próxima generación", en el numeral 6,23 Asuntos de interés público, establece:

"Las NGN ofrecerán las capacidades necesarias para la prestación de los servicios de interés general requeridos por la reglamentación o las leyes de autoridades regionales o

[29] Tratado del Atlántico Norte, sobre Cooperación y Seguridad de Información, 25 de junio de 2013 y promulgado a través de la ley 1734 de 8 de septiembre de 2014, fuente: http://apw.cancilleria.gov.co/tratados/SitePages/VerTratados.aspx?

nacionales, o conforme a tratados internacionales. Entre dichos servicios se cuentan los que se describen en las subcláusulas siguientes.

2.1.4.2. La interceptación legal

1) Un proveedor de transporte o de servicio NGN cumplirá con las exigencias de interceptación legal. Por tanto, las NGN proporcionarán los mecanismos que hagan posible dicha interceptación cuando una tal posibilidad esté requerida por los reglamentos o la ley de un país en la zona de aplicación.

2) Gracias a los mecanismos de interceptación legal, las autoridades podrán acceder al contenido de la comunicación e interceptar la información pertinente con arreglo a los requisitos de las administraciones y conforme a los tratados internacionales.

3) Tratándose de un aspecto que depende de las costumbres y de las leyes de cada país o región, los requisitos que ha de cumplir la interceptación legal son función del entorno reglamentario en cuestión[30] [14].

2.1.5. Compendio de Normas y Acuerdos internacionales

La tabla 3-2, presenta el consolidado de normas y acuerdos internacionales que Colombia, observa y/o aplica en materia de interceptación telefónica.

Es importante observar, que en el caso colombiano, nuestro país, por naturaleza, se acoge a los acuerdos internacionales, esto ha sido una práctica de costumbre, sin embargo la observancia y aplicación de estos acuerdos en algunos casos no es la costumbre de algunos gobiernos que han dispuesto su propio criterio en la aplicación de principios e interpretación de las normas y tratados internacionales, de acuerdo a intereses particulares o políticas del gobierno de turno. Esto de alguna forma ha dado origen a que en algunos casos, los mismos organismos de seguridad del estado, utilicen la interceptación como una herramienta para manipular y ejercer el poder sin la observancia de los principios y derechos fundamentales consagrados en cada una de las normas de nuestro país, en lo referente a la Intimidad, libre expresión y en general la reserva de la información.

[30] Rec-UIT-T Y.2201 (04/2007)

Tabla 2-2: Normas y Acuerdos Internacionales (parte 1)

Item	Tipo	Descripción	Fecha	O.B.S
1.	Acuerdo	Decreto 318	2008	Acuerdo entre el gobierno de la república de Colombia y el gobierno de la república Francesa relativo a la cooperación en materia de seguridad interior.
2.	Acuerdo	Organización del tratado del Atlántico Norte (OTAN)	Junio de 2013	Acuerdo entre la república de Colombia y la organización del tratado del atlántico norte sobre cooperación y seguridad de información
3.	Acuerdo	De cooperación en materia de Defensa con el Gobierno de la república federativa del Brasil.		El objetivo del Acuerdo es promover la cooperación entre las Repúblicas de Colombia y Brasil en materia de defensa, en especial en materia de investigación, apoyo logístico, industria aeronáutica, naval y terrestre, intercambio de conocimientos y experiencias y acciones conjuntas de entrenamiento, con el fin de fortalecer la capacidad de respuesta de las autoridades nacionales de ambos países e incrementar el intercambio de experiencias, experticia y fortalezas en las diferentes áreas
4.	Declaración	Declaración Universal de los derechos Humanos Art. 12.	10 de diciembre de 1948	Aplica a nivel Universal
5.	Pacto Internacional	Pacto Internacional de Derechos Civiles y Políticos Art. 17	16 de diciembre de 1966.	Resolución 2200 A (XXI) de la Asamblea General.
6.	Carta	Carta de la Unión Europea Art. 7.	7 de diciembre de 2000	El texto supra recoge, adaptándola, la Carta proclamada el 7 de diciembre de 2000, a la que sustituirá a partir del día de la entrada en vigor del Tratado de Lisboa.
7.	Convenio	Convenio Europeo de Derechos Humanos Art. 8	Junio de 2010	Abierto a la firma en Roma en 1950. Modificado en junio 01 de 2010 por el protocolo No. 14.

Tabla 2-3: Normas y Acuerdos Internacionales (Parte 2)

Item	Tipo	Descripción	Fecha	O.B.S
8.	Directiva	Directrices de la OCDE para la seguridad de sistemas y redes de información	25 de julio de 2002)	Hacia una cultura de Seguridad se adoptaron como Recomendación del Consejo de la OCDE en su sesión 1037
9.	Directiva	Directiva de la CEE	27 de septiembre de 1990	Relativa a la protección de datos personales y de la intimidad en el contexto de las redes digitales públicas de las telecomunicaciones y en particular de la red digital de servicios integrados y de las redes digitales móviles públicas (SYN 288).
10.	Sentencia	Caso Escher y Otros vs. Brasil	6 de julio de 2009	Corte Interamerica de derechos Humanos
11.	Directiva	Directiva 2006/24/CE del parlamento europeo y del consejo	15 de marzo de 2006	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE
12.	Convenio	Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH)	.	Artículo 8.- Derecho al respeto a la vida privada y familiar
13.	Ley	34 de 2002 [15]	11 de Julio	De servicios de la sociedad de la información y de comercio electrónico
14.	Ley	11/2002, , Reguladora del Centro Nacional de Inteligencia [16].	6 de mayo	Trata acerca de los servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional
15.	Recomendación	Recomendación UIT-T y. 2201 (04/2007) [14] Intercpetación Legal	Abril de 2007	Redes de la próxima generación – Aspectos relativos a los servicios: capacidades y arquitectura de servicios. Requisitos de las redes de la próxima generación, versión 1

2.2. Regulación en Colombia

2.2.1. Constitución Política de Colombia:

Artículo 15 [2]**:** "Todas las personas tienen derecho a su intimidad personal y Familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".

Como se puede leer, el artículo 15 establece tres derechos: **El derecho a la intimidad personal, derecho al buen nombre y el derecho a la información o habeas data.**

Respecto del derecho a la intimidad, mediante sentencia C-239 de 1997, la Corte constitucional señalo:

"los derechos fundamentales, no obstante su consagración constitucional y su importancia, no son absolutos y, por tanto, necesariamente deben armonizarse entre sí con los demás bienes y valores protegidos por la Carta, pues, de lo contrario, ausente esa indispensable relativización, la convivencia social y la vida institucional no serían posibles"

Esta posición de la corte da paso a la posibilidad de ajustar el derecho a la intimidad, bajo circunstancias específicas y reguladas por la ley, a fin de realizar seguimientos o actividades de inteligencia.

Artículo 28 [2]**:** "Toda persona es libre. Nadie puede ser molestado en su persona o familia, ni reducido a prisión o arresto, ni detenido, ni su domicilio registrado, sino en virtud de mandamiento escrito de autoridad judicial competente, con las formalidades legales y por motivo previamente definido en la ley".

Aquí, es importante llamar la atención respecto de la aplicación y la interpretación que hoy, tiene este artículo en el entendido que "Domicilio", puede tomarse como un lugar físico de habitación.

La real academia de la Lengua define Domicilio como: "Lugar en que legalmente se considera establecido alguien para el cumplimiento de sus obligaciones y el ejercicio de sus derechos".

Este concepto hoy a la luz del mundo actual ha cambiado, toda vez que este se puede incluir otros entornos, no solamente el lugar físico de habitación, casa o apartamento.

La evolución de las tecnologías de información y las comunicaciones, han permitido la convergencia de estas y de los servicios que se prestan a través de ellas. Así un domicilio también puede ser un lugar de trabajo desde el cual se tiene comunicación a diferentes partes del mundo, entonces es importante que la normatividad precise qué incluye hoy un domicilio, pues en este, además pueden tenerse redes y equipos de comunicaciones, cuya cobertura de acción supera la delimitación de lo que se puede entender como domicilio.

Por otra parte, la Constitución política faculta a la Fiscalía General de la Nación para realizar registros, allanamiento, incautaciones e interceptaciones de comunicaciones, sin orden judicial previa, y establece que se debe tener un control posterior sobre lo realizado.

Lo anterior está consagrado en el artículo 250 de la carta magna; “En ejercicio de sus funciones la Fiscalía General de la Nación, deberá: ... Adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones. En estos eventos el juez que ejerza las funciones de control de garantías efectuará el control posterior respectivo, a más tardar dentro de las treinta y seis (36) horas siguientes, *(al solo efecto de determinar su validez)*”

En cuanto a quienes están facultados por la norma para realizan los procesos de interceptación en Colombia, se tiene lo siguiente: “La legislación procesal penal también establece que “las autoridades competentes” serán las encargadas de la operación técnica de la interceptación y de su procesamiento. A pesar de la vaguedad de la ley en lo relativo a las autoridades encargadas de realizar la operación, la Corte Constitucional la avaló. El argumento que utilizó es que la norma sí especifica la autoridad que da la orden y dirige la interceptación (la Fiscalía General de la Nación), dejándole la posibilidad de determinar las autoridades que realizan la tarea de interceptación y su procesamiento. Además, aunque la norma no especifica estas “autoridades competentes”, pueden ser determinadas a través de una interpretación sistemática de las normas que regulan la operación técnica de la interceptación de comunicaciones. Señala la Corte que el artículo 46 de la ley 938 de 2004 establece que la mencionada competencia recae en las autoridades de policía judicial (actualmente, los órganos que cumplen funciones de policía judicial son el Cuerpo Técnico de Investigaciones y la Policía Nacional)”[31] [17].

2.2.1.1. En estado de conmoción interior

La Ley 137 de junio de 1994 [18], faculta al gobierno para interceptar las comunicaciones; al respecto indica: Articulo 38, literal e) “Disponer con orden de

[31] Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia Por Juan Camilo Rivera y Mayo 2015

autoridad judicial competente, la interceptación o registro de comunicaciones con el único fin de buscar pruebas judiciales o prevenir la comisión de delitos"[32].

2.2.2. Código de procedimiento penal

2.2.2.1. La interceptación de comunicaciones como delito

De otra parte la Interceptación de comunicaciones sin orden judicial, se tipifica como delito en el Código de Procedimiento Penal, en el Titulo VII bis, capítulo I DE LOS ATENTADOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y DE LOS SISTEMAS INFORMÁTICOS; al respecto el articulo 269 C dice: "el que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses".

2.2.3. Ley estatutaria 1621 del 17 de abril de 2013 "Ley de Inteligencia y contrainteligencia"

El estado con el fin de garantizar la seguridad de sus habitantes, sus entidades y de sí mismo, ha organizado y dispuesto estrategias al interior de los organismos de seguridad, para ello ha creado "grupos" de inteligencia y contrainteligencia cuyas funciones están normatizadas mediante la legislación, en este sentido se tiene la ley de inteligencia y contra inteligencia, que faculta a organismos de seguridad a realizar las actividades tendientes a contrarrestar la comisión de hechos en contra de las personas u organizaciones. De esta manera se determinan las siguientes funciones, que de alguna manera llegan a limitar los derechos de las personas:

Artículo 17. Monitoreo del espectro electromagnético e interceptaciones de comunicaciones privadas.

Establece que esta actividad solo podrá desarrollarse en ejercicio de "órdenes de trabajo de operaciones o misiones de trabajo", y que la información que no sea benéfica para los objetivos de inteligencia debe ser destruida.

Un segundo aspecto está relacionado con la obligación que tienen los operadores de servicios de telecomunicaciones; el artículo 44 "Colaboración con operadores de servicios de telecomunicaciones"; establece que "Los operadores de servicios de

[32] Ley 137 de 1994. Disponible en http://wsp.presidencia.gov.co/Normativa/Leyes

telecomunicaciones estarán obligados a suministrar a los organismos de inteligencia y contrainteligencia, previa solicitud y en desarrollo de una operación autorizada y siempre que sea técnicamente viable, el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recae la operación, así como la localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización. ... limitarán la información solicitada a un período que no exceda de cinco (5) años. Los Directores de los organismos de inteligencia, o quienes ellos deleguen, serán los encargados de presentar por escrito a los operadores de servicios de telecomunicaciones la solicitud de dicha información. En todo caso, la interceptación de comunicaciones estará sujeta a los procedimientos establecidos por el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrá llevarse a cabo en el marco de procesos judiciales"

A su vez el decreto 1704 [19] de 2012, que reglamenta el artículo 52 de la ley 1453 de 2011, "Interceptación de comunicaciones". Indicando la obligación de los operadores de servicios de telecomunicaciones que tienen para facilitar los medios tecnológicos y el acceso a las bases de datos, fin obtener la información de los objetivos de la investigación y/o seguimiento. De la misma forma, establece que los operadores tienen la obligación de conservar la información de los subscriptores por un término de 5 años. Esta obligación causa polémica, toda vez que el almacenamiento de la información es en forma discriminada, es decir de todos los usuarios, sin necesidad que exista investigación previa. Por supuesto la ley, justifica esta acción en la *seguridad nacional* [33]

Por su parte la ley de inteligencia en su artículo 44, justifica cuando los organismos de seguridad del estado pueden requerir a las empresas de telecomunicaciones información de sus usuarios, sin embargo no hace claridad en el tipo de información, dando lugar a "toda la información de los subscriptores. En resumen todos los ciudadanos de Colombia, somos en todo momento potenciales objetivos de los sistemas de interceptación telefónica, por seguridad Nacional.

El decreto 857 [20]de 2014, establece los organismos y dependencias que están facultados para realizar actividades de inteligencia y contrainteligencia así:

a) En las Fuerzas Militares:

- En el Comando General de las Fuerzas Militares:
  La Jefatura de Inteligencia y Contrainteligencia Militar Conjunta, sus Direcciones, Divisiones y/o equivalentes y demás unidades o dependencias de inteligencia y contrainteligencia subordinadas a ella.

[33] Decreto 1704 de 2012

- Las unidades o dependencias de inteligencia y contrainteligencia en cada uno de los Comandos Conjuntos o Comandos de Fuerza de Tarea conjunta.
- Las unidades o dependencias especiales creadas por el Comandante General de las Fuerzas Militares, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia y Contrainteligencia Militar Conjunta, de acuerdo con su misión, competencias y funciones.

b) En el Ejército Nacional:

- La Jefatura de Inteligencia y Contrainteligencia del Ejército Nacional, las dependencias y unidades de inteligencia y contrainteligencia subordinadas a ella.

- Las dependencias de inteligencia y contrainteligencia en cada División, Brigada, Batallón y unidades que por su naturaleza y misión desarrollen estas actividades en sus diferentes niveles.

- Las unidades especiales creadas por el Comandante del Ejército, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia y Contrainteligencia Militar, de acuerdo con su misión, competencias y funciones.

c) En la Armada Nacional:

- La Jefatura de Inteligencia Naval, las dependencias y unidades de inteligencia y contrainteligencia subordinadas a ella.
- Las dependencias de inteligencia y contrainteligencia en cada una de las unidades de la Armada Nacional, que por su naturaleza, misión y organización desarrollen estas actividades en sus diferentes niveles.

- Las unidades especiales creadas por el Comandante de la Armada Nacional, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia Naval, de acuerdo con su misión, competencias y funciones.

d) En la Fuerza Aérea Colombiana:

- La Jefatura de Inteligencia Aérea, las dependencias y unidades de inteligencia y contrainteligencia subordinadas a ella.

- Las dependencias de inteligencia y contrainteligencia en cada una de las unidades de la Fuerza Aérea Colombiana, a nivel estratégico, operacional y

táctico, que por su naturaleza y misión desarrollen estas actividades en sus diferentes niveles.

- Las unidades especiales autorizadas por el Comandante de la Fuerza Aérea Colombiana, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia Aérea, de acuerdo con su misión, competencias y funciones.

e) En la Policía Nacional:

- La Dirección de Inteligencia Policial con sus dependencias subordinadas, la cual dirigirá, coordinará e integrará la función de inteligencia y contrainteligencia en la Policía Nacional.

- Los grupos especializados de la Policía Nacional que sean creados por el Director General de la Policía Nacional, previo concepto de la Dirección de Inteligencia Policial, de acuerdo con su misión, competencias y funciones.

f) En el Departamento Administrativo "Dirección Nacional de Inteligencia"
- Todas las dependencias orgánicas a ella.

g) En la Unidad de Información y Análisis Financiero (UIAF)
- Todas las dependencias orgánicas a ella.[34]

A nivel internacional, la Unión europea tiene normas, ajustadas en el tema de interceptación telefónica, esto demuestra la importancia del tema a nivel mundial. Toda vez que como herramienta coadyuva en los procesos de prevención, mitigación y acción contra el delito.

Sin embargo, es bien sabido que las tecnologías de interceptación, no solamente se han usado con propósitos acorde a las normas, sino también para fines e intereses personales violando los derechos humanos de las personas. Aun así la interceptación de comunicaciones es un proceso aceptado y reconocido en el mundo. Esto está demostrado al ser incluido en las leyes de los diferentes países, por ello es importante que se encuentre muy bien delimitado sus procedimientos, y al mismo tiempo se ajuste a los nuevos desarrollo tecnológicos.

En cuanto al tiempo de conservación de la información de los subscriptores, la Corte Europea de justicia, a través de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, en el artículo 6, “Períodos de conservación”, establece los tiempos mínimos y

[34] Decreto 857 de 2014

máximos para este proceso: “Los Estados miembros garantizarán que las categorías de datos mencionadas en el artículo 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación”.

Lo anterior contrasta los tiempos en Colombia, los cuales son de cinco (05) años, en la conservación de información. En este sentido además es importante conocer en qué casos y/o condiciones se realiza el proceso de interceptación de las comunicaciones en nuestro país. Al respecto el artículo 235 de la ley 906 de 2004, establece las condiciones en las que el juez, podrá ordenar la interceptación de comunicaciones así:

“**Interceptación de comunicaciones telefónicas y similares**. El fiscal podrá ordenar, con el único objeto de buscar elementos materiales probatorios y evidencia física, que se intercepten mediante grabación magnetofónica o similar las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación. En este sentido las entidades encargadas de la operación técnica de la respectiva interceptación, tienen la obligación de realizarla inmediatamente después de la notificación de la orden. En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva. Por ningún motivo se podrá interceptar las comunicaciones del defensor. La orden tendrá una vigencia máxima de tres (3) meses, pero podrá prorrogarse hasta por otro tanto si, a juicio del fiscal, subsisten los motivos fundados que la originaron”.

Siguiendo con el análisis del proceso de interceptación de las comunicaciones, conforme al código de procedimiento penal, este a través de los artículos 237 y 238 faculta a las personas objeto de interceptación, para que puedan conocer los resultados del seguimiento, y de esta forma una vez hayan sido imputados de cargos o antes, poder intervenir en proceso o solicitar audiencia para pedir la exclusión de las evidencias y o pruebas que se les indilguen.

Ahora bien en el caso de la ley de inteligencia y contrainteligencia, no existe la anterior posibilidad, es decir que una persona pueda conocer si es o ha sido objeto de seguimiento por parte de algún organismo de inteligencia. Y por supuesto que no lo puede hacer, entonces no sería una labor de inteligencia. Pues un delincuente estaría prevenido de las acciones del estado.

Es entonces necesario aclarar o indicar cuales son los alcances de la normativa ley 906 y los de la ley de inteligencia, pues una y otra son vigentes en todo momento en Colombia mientras, la autoridad competente no aplaza o interrumpa por un periodo de tiempo su acción.

2.2.4. Consecuencias de las interceptaciones Telefónicas en Colombia

Las consecuencias de las interceptaciones telefónicas se pueden enunciar en dos sentidos: Positivas y negativas:

2.2.4.1. Las Positivas

Hacen referencia a los aportes que ha contribuido esta herramienta tecnológica en acciones contra el delito nacional y transnacional, para este efecto no se van a citar cada uno de los delitos o acciones criminales en las cuales se han obtenido buenos resultados gracias al uso de interceptación, pues está más allá del alcance de este documento; el referido a las leyes. En procura de examinar las bondades de la interceptación seguidamente se citan casos relevantes donde sin esta, no hubiese sido posible alcanzar los resultados obtenidos.

Otro aspecto importante que se debe analizar es el entorno de las normas que han contribuido a mejorar los procedimientos de la interceptación telefónica. Es claro que este tema causa polémica en todas partes del mundo, sin embargo cada vez más, se utilizara para contrarrestar los delitos y asegurar la Seguridad Nacional de los estados y prevenir o mitigar las acciones que pongan en peligro la vida honra y bienes de las sociedades.

Como se enuncio antes, un país no está solo en la lucha contra el delito y tampoco es autónomo para emplear las herramientas que considere en busca de un objetivo sin observar normas internacionales en especial las referidas a los derechos humanos.

En el caso Colombiano, la Comisión Interamericana de Derechos Humanos, en 2009, le manifestó su preocupación a Colombia acerca de las garantías que debían observarse sobre las personas que eran vigiladas tecnológicamente; al respecto en el capítulo IV párrafo 136, del “Informe anual de la Comisión Interamericana de Derechos Humanos 2009” [21] se reconoce que mediante la ley 1288 de 2009 [22], se expiden normas para fortalecer el marco legal, que le permite a los organismos de seguridad del estado, realizar actividades de inteligencia y contrainteligencia, y a su vez fortalece y “crear nuevas garantías para los ciudadanos, la reserva de la información y la protección de los funcionarios que desarrollan estas actividades”.

Se indica que el estado colombiano con esta ley, realiza una reestructuración de los servicios de inteligencia y contrainteligencia. Seguidamente en el párrafo 137, advierte a Colombia indicando:

“Sin embargo, la Comisión ha recibido información en la que se establece la falta de idoneidad de la Ley de Inteligencia (Ley 1288 de 2009 [22]) para la “erradicación de la

grave situación de riesgo en la que se encuentran las defensoras [y] defensores [de derechos humanos,] y líderes sociales perseguidos y hostigados por los organismos de inteligencia, […] no sólo por la insuficiencia de las declaraciones de principios y la ausencia de mecanismos para hacerlos efectivos, sino porque […] refuerza los mismos esquemas que han dado lugar a los desmanes de los organismos de seguridad" [23]. Concretamente, preocupa a la Comisión la ausencia de mecanismos para que las personas sobre quienes existe información de inteligencia tengan acceso a ella y de esa forma puedan solicitar su corrección, actualización o en su caso la depuración de los archivos de inteligencia. Asimismo, la Comisión ha tomado conocimiento sobre el desarrollo de investigaciones clandestinas contra defensores y defensoras de derechos humanos. Se ha señalado que "[d]os de los aspectos distintivos de los casos en contra de defensores son el uso de testimonio falso de excombatientes y el uso de archivos de inteligencia inadmisibles" [24].

"...En septiembre de 2009 la Relatora de Naciones Unidas sobre la Situación de Defensores de Derechos Humanos, Margaret Sekaggya, realizó una visita a Colombia. En declaraciones al término de su visita concluyó que "siguen existiendo en Colombia patrones de hostigamiento y persecución contra los defensores de derechos humanos, y a menudo contra sus familiares […] [a]l parecer, algunas de estas violaciones hay que atribuirlas a miembros de la guerrilla, a nuevos grupos armados ilegales y a grupos paramilitares que, según los defensores de derechos humanos, no han sido desmantelados". Señaló también que "[u]n motivo fundamental de la inseguridad de los defensores de derechos humanos radica en la estigmatización y el señalamiento sistemáticos de que son objeto por parte de funcionarios del Gobierno"[35] [21].

2.2.4.2. Las negativas.

Las actividades ilegales realizadas por el Departamento Administrativo de Seguridad (DAS). En su momento hizo que en este sentido la CIDH, indicará su preocupación: "la Comisión se encuentra aun gravemente preocupada y continuará dando seguimiento a las medidas destinadas al esclarecimiento judicial de los hechos, al establecimiento y mandato que se otorgue a la nueva agencia de inteligencia y al cese definitivo de dichas actividades ilegales por parte de todas las agencias del Estado"[36].

Hoy para nadie es un secreto que los gobiernos invierten gran parte del presupuesto de las naciones en la adquisición e implementación de nuevas tecnologías que la industria comercial ofrece afín de satisfacer las necesidades de estados en mejorar sus capacidades de vigilancia, haciéndolas cada vez más expansivas e intrusivas.

---

[35] Informe anual de la Comisión Interamericana de Derechos Humanos 2009, documento OEA- Capítulo IV, párr. 137, y 13. fuente: <http://www.cidh.oas.org/annualrep/2009sp/cap.4Colo.09.sp.htm>
[36] Ibídem; párrafo 140

"Se calcula que la industria de la vigilancia se valoraba en alrededor de 5.000 millones de dólares en 2011, y crece un 20 por ciento al año[37]".

Tabla 2-4: Normas de Interceptación telefónica en Colombia

Nro.	Tipo	Nro.	Nombre	Descripción
1	Constitución política de Colombia	N/A	Articulo 15 Artículo 250, numeral 2 (para investigación criminal)	Establece los derechos a la intimidad y a la libre expresión
2	Ley 906	Ley 906 de 2004	Código de procedimiento penal Arts. 235 y ss. Decreto 1704 [19]de 2012.	Define el concepto de interceptación telefónica y en qué casos se da
3	Ley Estatutaria Nº1621[38]	de 17 de abril de 2013	Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal.	Especialmente los artículos 17 y 44.
4	Decreto	1630 del 19/05/2011	Por medio del cual se adoptan medidas para registrar la operación de equipos terminales hurtados que son utilizados para la prestación de servicios de telecomunicaciones móviles"	Obliga al registro de la SIM, asociada a la identificación de una persona.
5	Ley 137 de 1994 [18]	Junio 2 de 1994	Por la cual se regulan los Estados de Excepción en Colombia	Concede atribuciones especiales a los organismos de seguridad del Estado.
6	Ley 1341 de 2009	1341	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC.	Crea la Agencia Nacional del Espectro y se dictan otras disposiciones

[37] Ibídem
[38] http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

Nro.	Tipo	Nro.	Nombre	Descripción
7	Decreto	1704 del 15/08/2012	Por medio del cual se reglamenta el artículo 52 de la Ley 1453 de 2011, se deroga el Decreto 075 [25] de 2006 y se dictan otras disposiciones.	Artículo 2. (parágrafo); faculta al ministerio de las TIC para hacer esa regulación
8	Decreto	857 [20] de 2014	Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013,	Se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones
9	Ley	1273 de 2009 [26]	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"-	Se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

"La regulación de la vigilancia de las comunicaciones por la autoridad es un asunto de gran sensibilidad en el contexto colombiano, debido a los múltiples casos de repercusión pública ocurridos en años recientes con relación a este tema. Entre ellos se cuenta, por ejemplo, las arbitrariedades que de manera sistemática y generalizada fueron cometidas por los servicios de inteligencia entre los años 2003 y 2008, los cuales fueron utilizados para perseguir y vigilar periodistas, miembros de partidos de la oposición, defensores de derechos humanos, magistrados de las Altas Cortes, y, en general, personas que pudieran ser consideradas opositoras a las políticas gubernamentales..."[39]

De acuerdo con este tribunal, para que una injerencia no se considere arbitraria o abusiva debe a) estar prevista en ley, b) perseguir un fin legítimo, y c) ser idónea, necesaria y proporcional [24]. Estas limitaciones han sido definidas de manera general por la Corte Interamericana, pero pueden precisarse acudiendo a lo dispuesto por la Corte Europea de Derechos Humanos. Esta última ha señalado, entre otras, que las medidas de vigilancia deben basarse en una ley que sea particularmente precisa,

[39] "Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia"

principalmente por el riesgo implícito de abuso de cualquier sistema de vigilancia secreta y por la continua sofisticación de la tecnología disponible para realizar esas actividades. [25] Así, no serían suficientes autorizaciones de vigilancia generales y vagas contenidas en una ley para entender que se satisface el criterio de legalidad.[40]

[40] Ibídem.

3. Estudio y análisis de las tecnologías de interceptación telefónica

La constitución política de Colombia, en el artículo 15 [2]; establece que "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar… La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley".[41] Dando vida a los procedimientos de interceptación y registros de información, bases de datos y diferentes modos de comunicación como la vía telefónica.

Los procedimientos técnicos empleados para la interceptación telefónica están amparados en normas y manuales avalados por las entidades judiciales correspondientes[42].

3.1. Procedimiento para la interceptación telefónica

El código de procedimiento penal (CPP), define la actuación que deben observar los funcionarios que ejecutan este procedimiento, así en el artículo 14 del Código, establece con respecto a la Intimidad: "Toda persona tiene derecho al respeto de su intimidad. Nadie podrá ser molestado en su vida privada. NO podrán hacerse registros, allanamientos ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o su delegado… De la misma manera deberá procederse cuando resulte necesaria la búsqueda selectiva en las bases de datos computarizadas, mecánicas o de cualquier otra índole, que no sean de acceso, o cuando fuere necesario interceptar comunicaciones" [27].

---

[41] Constitución política de Colombia, articulo 15. Pág. 3.
[42] Ley 906 del 31 de agosto de 2004. Art. 14. Intimidad.

El articulo 146 Registro de la actuación, del CPP, indica el procedimiento y los medios habilitados para realizar la interceptación, a la letra dice: “se dispondrá el empleo de los medios técnicos idóneos para el registro y reproducción fidedignos de lo actuado, de conformidad con las siguientes reglas…1. En las actuaciones de la Fiscalía General de la Nación (FGN) o de la Policía Judicial que requieran declaración juramentada, conservación de la escena de hechos delictivos, registro y allanamiento, interceptación de comunicaciones o cualquier otro acto…será registrado y reproducido mediante cualquier medio técnico que garantice su fidelidad, genuinidad u originalidad.[43]

En el caso Colombiano los organismos autorizados para realizar estos procedimientos son aquellos que además de tener facultades de Policía Judicial, han sido determinados mediante mandato de la F.G.N. En tal sentido el manual de procedimientos de la Fiscalía en el Sistema penal acusatorio establece que la “interceptación de comunicaciones telefónicas y similares”, Es una diligencia de carácter reservado ordenada por el fiscal delegado y practicada por servidores de policía judicial, orientada a captar por medio de grabación magnetofónica o similar información que fluya a través de comunicación telefónica, radiotelefónica u otra técnica que utilice el espectro electromagnético, para obtener elementos materiales probatorios o evidencia física de interés para la investigación. (2)

Al interior de la Policía Nacional se tiene una estructura Orgánica que define la jerarquía y áreas específicas de los procesos. La estructura se muestra en la figura 4-1

3.1.1. Proceso de la interceptación telefónica

Los pasos que a continuación se enumeran no pueden ni deben corresponder al proceso estricto toda vez que este es confidencial, sin embargo es un acercamiento y visión general obtenida de diferentes fuentes públicas, citadas en cada caso.

Paso 1: Se inicia con la Fuente, la cual puede ser de diferentes tipos:

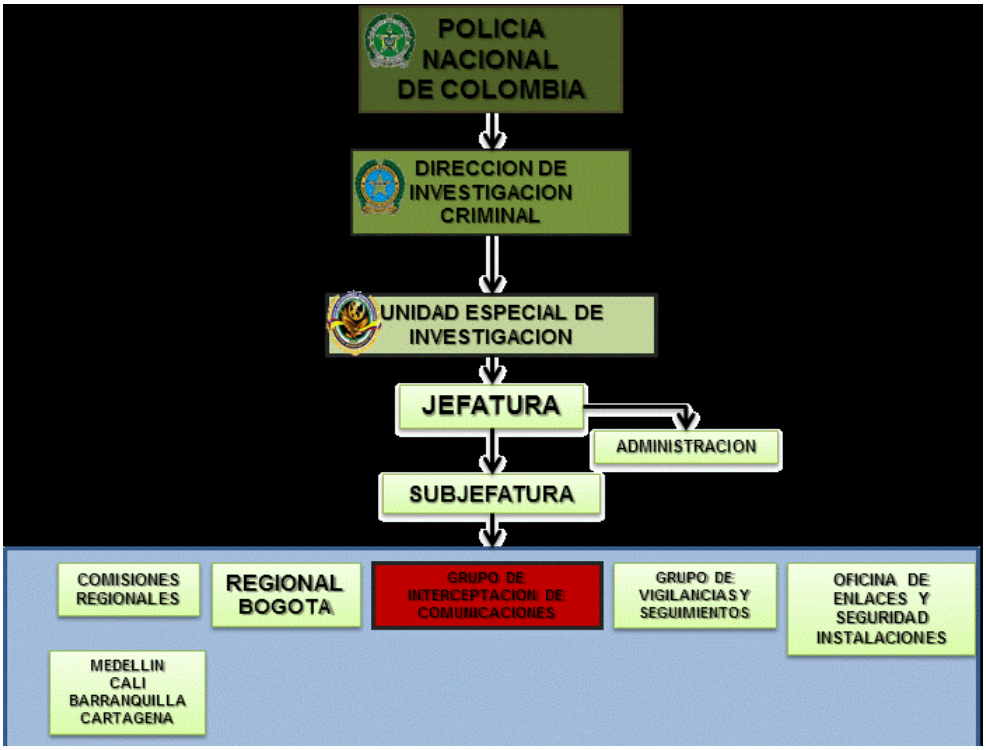
a) Formales

- ✓ Denuncia. La presenta cualquier persona natural o el representante legal de una persona jurídica afectada.
- ✓ Petición especial del Procurador General de la Nación.
- ✓ Querella de la víctima o directamente perjudicado, su representante legal o herederos; del defensor de familia o del agente del Ministerio Público, según el caso.

[43] Ibídem 3. Articulo 146.

- ✓ Cualquier otro medio de origen oficial como informes de policía o de otra autoridad que haya tenido conocimiento de la ocurrencia de un hecho de probable connotación delictiva.

Figura 3-1: Estructura Orgánica de la Policía Nacional para el Proceso de interceptación telefónica



b) No formales

- ✓ Información obtenida por llamadas telefónicas, noticias difundidas por medios de comunicación, anónimos, informantes y correo electrónico, a manera de ejemplo. (2)

Paso 2: Se comunica al coordinador del Grupo y se realiza la valoración, análisis y cruce de información con el fin de determinar la veracidad de esta, lo que permite continuar el trámite o no.

Paso 3: Se realiza la solicitud a la Fiscalía. Es en este punto donde inicia en si el proceso mediante la orden de interceptación por parte del fiscal correspondiente, quien se toma un plazo de 24 a 48 horas para impartir la orden.

Paso 4: Orden del Fiscal. De conformidad con el artículo 235 de la ley 906 de 2004, el Fiscal podrá ordenar la interceptación de telecomunicaciones para lo cual se diligencia el formato 002, este documento se entrega al coordinador de la Sala.

Paso 5: Radicación ante el sistema de Interceptación. Una vez los coordinadores de la sala de Policía Judicial verifican la información contenida en el formato 002, se da paso a su radicación ante el Sistema de Interceptación, donde se realiza la programación de conformidad con lo ordenado por el Fiscal.

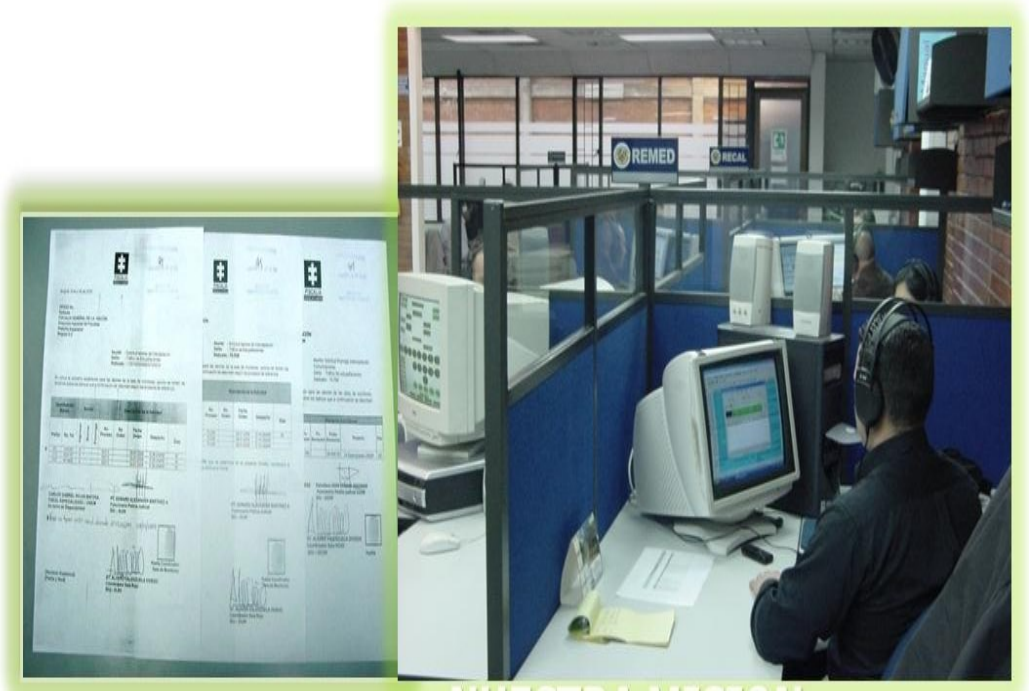
Paso 6: Ingreso de la línea al Sistema de Interceptación, esta función corresponde al programador del Sistema de Interceptación, quien ingresa el número o números solicitados y envía la señal a la sala o salas de escucha (grabación) correspondientes. En caso que algún número sea rechazado por el Sistema debido a que está siendo objeto de grabación en otra sala, el programador debe dar aviso inmediato al Coordinador de la Sala, quien a su vez informará a los solicitantes de dicho procedimiento.

El programador del Sistema tiene un plazo menor a doce (12) horas para realizar la actividad.

Para todo evento, la información recibida y originada será canalizada únicamente a través de los coordinadores titulares o suplentes de la sala de monitoreo. (ver figura 4-2).

Paso 7: Materialización de la Interceptación Telefónica. La señal de la línea (s) llega a la sala definida, donde el operador tiene acceso a nivel nacional, allí se programa en aplicativo determinado, o Base de Datos, acceso que tiene una clave conocida únicamente por el operador de la sala, quedando enrutada al analista.

Figura 3-2: Sala de Investigación Electrónica



Paso 8: Funciones del coordinador de la sala. Entre otras;

- ✓ Informar por escrito al Jefe de la sala la fecha en que se hizo la interceptación.
- ✓ Realiza la programación de la línea en la Base de datos y está atento a la labor de los analistas.
  - ✓ Gestionar la solución de fallas técnicas y en general cualquier requerimiento que sea necesario para garantizar el buen funcionamiento de la sala, esta gestión se hace ante el gerente técnico del proyecto.
  - ✓ Informar al jefe de la sala toda situación, para que este lo comunique al investigador a fin de toma de decisiones.

Paso 9: Prorroga de Interceptaciones telefónicas.

- ✓ Los analistas cumplen una función definitiva en la solicitud o no de una prorroga en el tiempo que se debe mantener interceptada una línea, en virtud de esto debe existir una intercomunicación permanente con el investigador a fin de inferir la necesidad. La cual debe estar soportada a través de informes temporales; mínimo cada 10 días, dirigidos al coordinador de la sala, quien a su vez revisa, evalúa y remite al Fiscal, autoría que autoriza o no la prórroga.

- ✓ El analista[44], entre otras funciones debe:

- Estar atento a los tiempos que dura la interceptación Telefónica, informar oportunamente al investigador los resultados y observaciones que se vayan obteniendo durante el proceso de la interceptación, en todo caso el informe técnico judicial que se presente ante el fiscal será competencia del Investigador quien cuenta con la funciones de Policía Judicial.
- Generar y cuidar la documentación que soporta legalmente el procedimiento, consistente en: Copia de la orden de interceptación expedida por el Juez o autoridad competente, copia del formato 002 radicado en el Sistema de Interceptación e informe de Policía Judicial que evidencia la necesidad de la interceptación.
- Realizar el control de las condiciones legales de los procedimientos que le hayan sido asignados.
- Verificar e informar oportunamente al profesional o administrador de sistemas de los problemas técnicos que lleguen a presentarse con las líneas telefónicas interceptadas.
- Pedir al Administrador del sistema de Interceptación originar las evidencias obtenidas durante el proceso de grabación aplicando los controles establecidos para este fin.
- Garantizar la seguridad de la información generada mediante la interceptación de comunicaciones.
- El uso de usuarios y contraseñas que utilizan los analistas debe cumplir con los protocolos de seguridad informática.
- La comunicación que en desarrollo de la actividad se realice entre analista e investigador deberá utilizar los medios seguros que garanticen el intercambio de información en forma precisa, clara y concisa de los hechos, sin riesgo de fugas de esta.
- Los análisis e informes que se hagan de las interceptaciones deben ser de conocimiento directo de los investigadores relacionados con el plan metodológico establecido por el ente Investigador, en forma oportuna para la toma de decisiones que permitan fortalecer la investigación mediante evidencias físicas y material probatorio.
- Los resultados de las interceptaciones deberán ser suministrados, por medio seguro a los investigadores de acuerdo al plan metodológico, para que estos informen o respondan oportunamente al Fiscalía.
- El informe que se realiza, está sujeto al Manual de Policía Judicial, y la entrega o envío de información debe regirse a los parámetros establecidos para cada sala de monitoreo y será de conocimiento exclusivo de los funcionarios que hagan parte del plan metodológico.

[44]Analista: funcionario con funciones de policía Judicial, usuario de una sala de interceptación de comunicaciones, primer responsable de interpretar las comunicaciones interceptadas. (2)

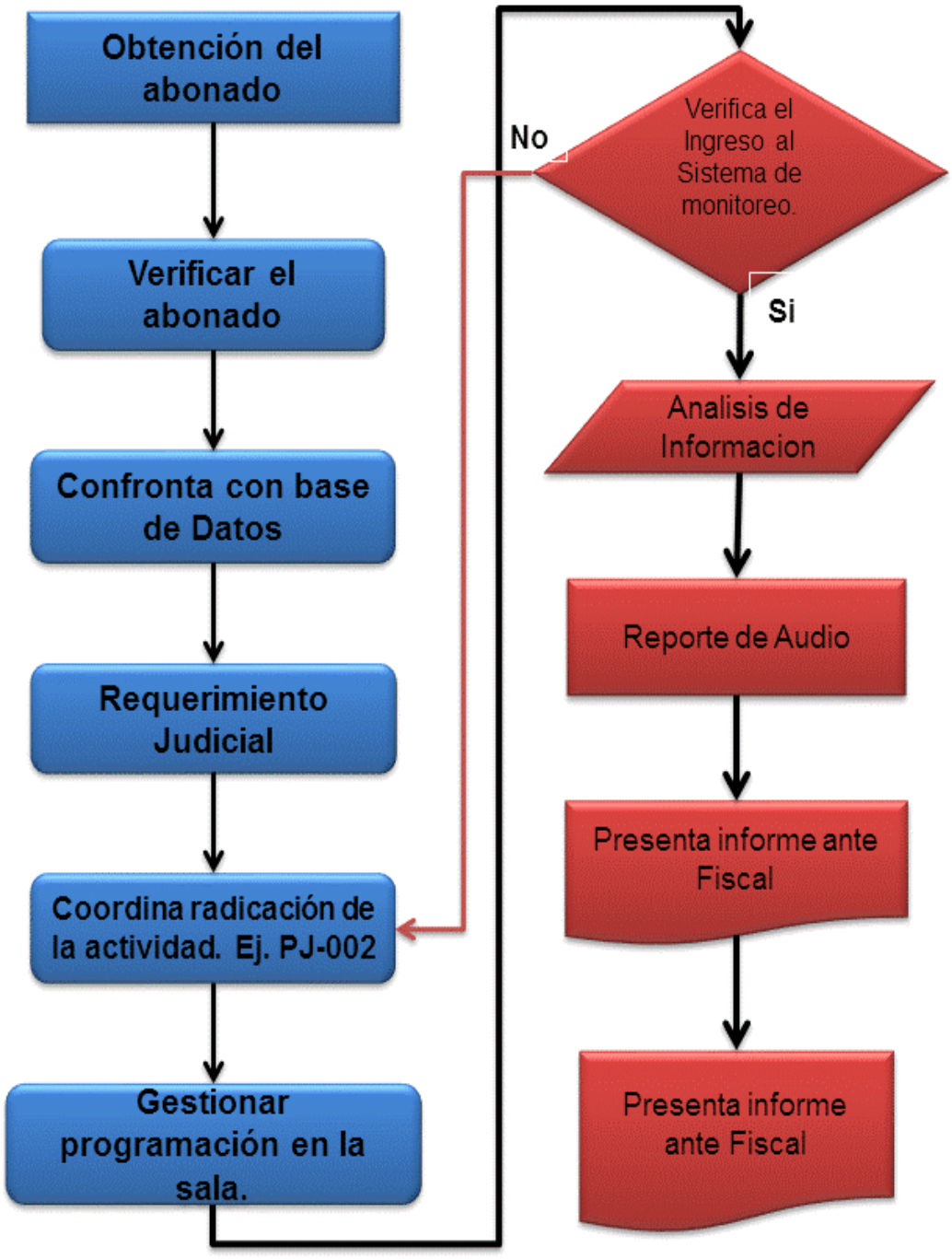
En resumen el, proceso de análisis comprende recurso humano y técnico, puede estar integrado por una persona o más, depende de la sala, el recurso tecnológico consta de herramientas de hardware y software, algunas de ellas tiene algunos años de uso, otras son de tecnología de punta, dispositivos electrónicos, software spia, bases de datos, infraestructura de telecomunicaciones. El resultado del análisis de información es en muchos casos la prueba reina de una investigación, en consecuencia esta demanda la máxima rigurosidad técnica y científica.

Aquí es muy importante tener en cuenta que hay dos tipos de información que se pueden obtener a través de las salas de interceptación; una es la información obtenida como seguimiento e interceptación a líneas o abonados telefónicos específicos, en cumplimiento a una orden judicial previa, cuya actuación hace parte de un proceso de investigación que adelantan las autoridades competentes, en este caso hay una trazabilidad judicial y todo el proceso debe estará bajo una cadena de custodia en cada una de sus actuaciones.

Este proceso está representado debidamente a través del diagrama de flujo de la siguiente figura. Donde se indican cada una de las funciones específicas:

Otra información es la de “Inteligencia”, que más adelante se trata en el documento.

Figura 3-3: Funciones de los analistas



3.2. Salas de Interceptación telefónica

Espacio o lugar oficial debidamente preparado y acondicionado con la infraestructura física tecnológica requerida para la recepción y análisis de las comunicaciones interceptadas por el Sistema de Interceptación.

El Gobierno Nacional a través de los grupos de seguridad del estado tiene establecidos unos puntos estratégicos para ejercer el proceso de interceptación, en la figura 2.3. Se presenta el esquema general de las regiones del País donde se sabe existen salas de monitoreo.

3.2.1. Seguridad de las salas de interceptación de comunicaciones

Deben disponer de áreas independientes dotadas de los acondicionamientos técnicos que garanticen el buen funcionamiento de los equipos de cómputo (servidores), también disponer de los espacios de trabajo de analistas y visitantes.

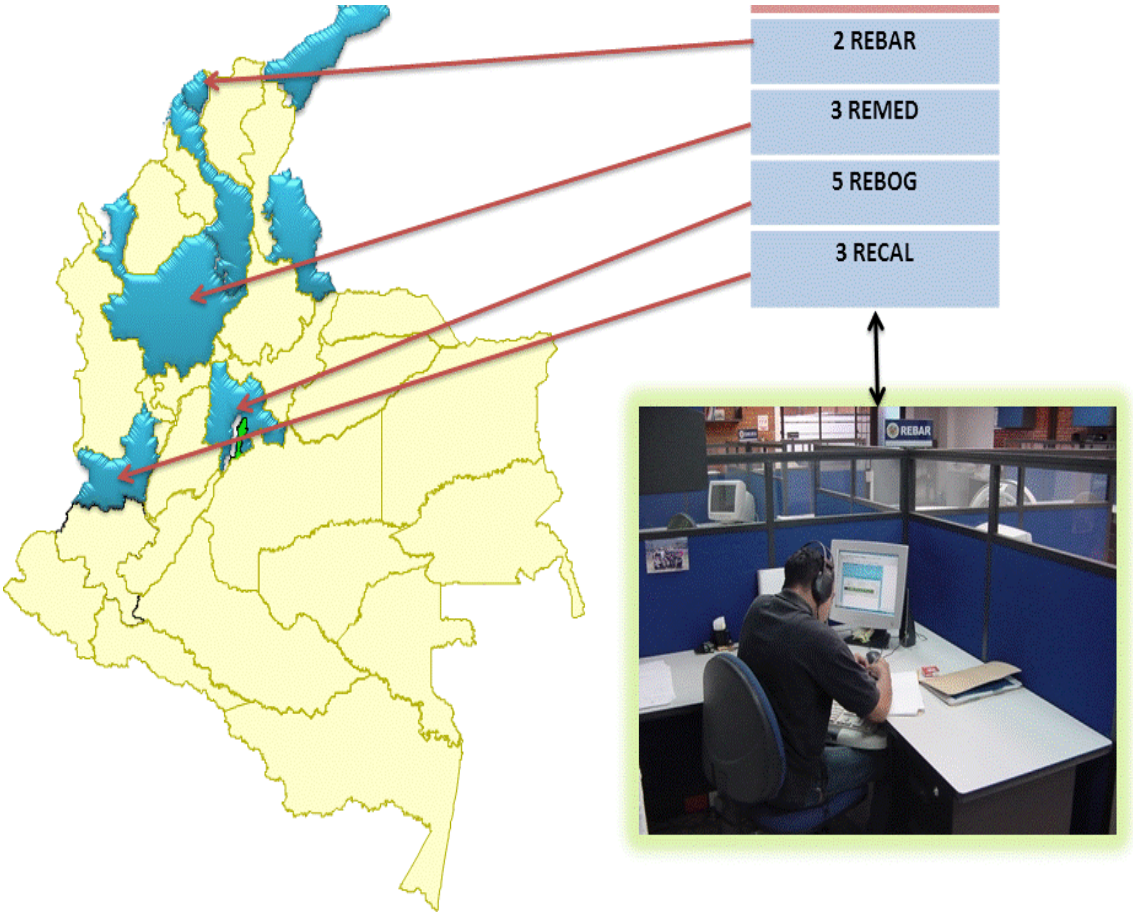
3.2.1.1. Sistemas electrónicos de seguridad.

Deben contar con al menos los siguientes:

- Control de acceso biométrico, con las debidas medidas de aseguramiento del equipo de grabación y su backup de registros.
- Control de acceso biométrico al centro de cómputo, allí deben existir los niveles de seguridad establecidos y los protocolos para backup de la información.
- Si la sala se encuentra fuera de instalaciones oficiales ejemplo la Policía Judicial, se debe disponer de un sistema de alarma con servicio de monitoreo.
- Sistema de grabación de video del acceso a la sala y al centro de cómputo donde se evidencie el monitoreo del sitio al 100%.
- Las salas deben estar dotadas de las herramientas y mecanismos, visuales, etc. que demandan las normas de seguridad industrial para centros de cómputo y oficinas.

La figura 3-4, Muestra la distribución de salas de interceptación, existente a mediados de 2012, sin embargo como se muestra más adelante en el análisis de las tecnologías, en la actualidad este número ha aumentado, como consecuencia de altas inversiones por parte del Gobierno para garantizar la Seguridad del estado.

Figura 3-4: Salas de monitoreo existentes en Colombia- distribución por regiones



4.2.1.2. Seguridad de la Información.

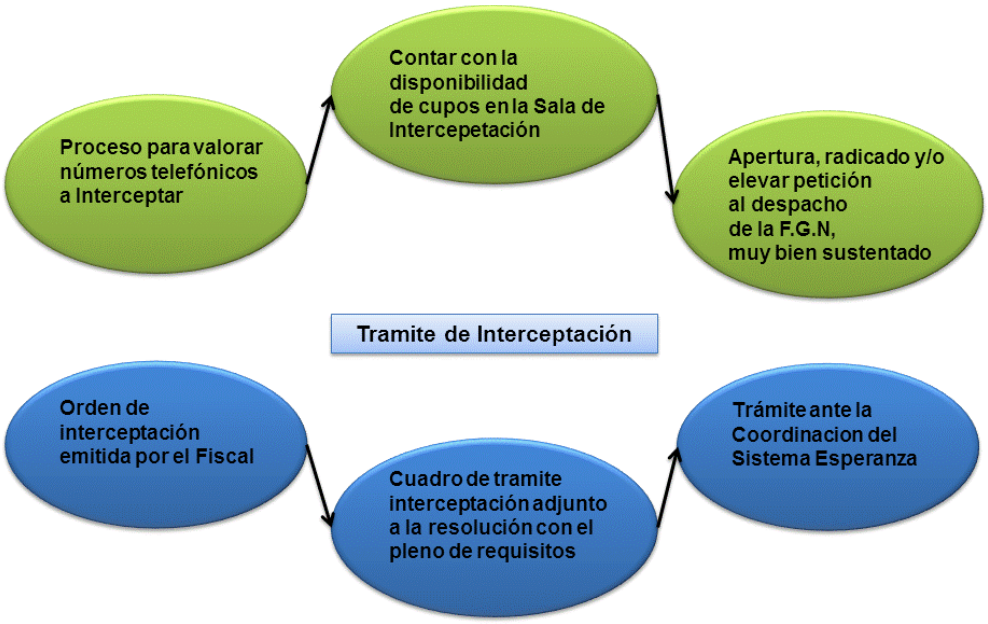
Se deben observar y cumplir obligatoriamente los siguientes criterios:

- Todo el software que se utilice en las salas debe ser licenciado.
- Todos los equipos que se conecten a la red de la sala deben tener antivirus con actualización permanente.
- Está prohibido el ingreso de dispositivos externos de almacenamiento ejemplo: Unidades de disco externas, USB, quemadores, celulares, videograbadoras, etc.
- Establecer políticas adecuadas para el manejo de usuarios y contraseñas.
- Se debe tener políticas de acceso en caso que sea necesario el ingreso de equipos celulares, computadores y cualquier otro tipo de dispositivo que permita conexión a la red de la sala de interceptación.
- Se debe tener bloqueado el acceso inalámbrico de cualquier dispositivo a la red de datos de la sala.
- Las estaciones de trabajo, servidores y equipos de cómputo que operen en la sala no tendrán conexión a internet.

- Cuando sea necesaria una conexión remota de la Sala se hará a través de VPN con los niveles de seguridad mínimos establecidos por el comité técnico del Sistema de Interceptación.

La siguiente figura muestra el proceso general que se efectúa como procedimiento previo y trámite de la interceptación.

Figura 3-5: Proceso de la información.



Cada una de las etapas de la figura anterior tiene definido un proceso, el cual en forma general y atendiendo a la reserva de información clasificada, consiste en: La valoración de números telefónicos, comprende la verificación de evidencia, la priorización de casos, la clasificación de fuentes y el impacto a la seguridad, a la sociedad, a la economía, entre otros. Disponibilidad de cupos; de acuerdo con la ubicación geográfica del "objetivo", la reserva e importancia del caso, se destina una sala específica, las interceptaciones de bajo perfil entran a "cola de espera", hasta que haya disponibilidad, otros aspectos que se valoran para asignar la sala son la priorización en el tiempo para obtener evidencia que pruebe ante la ley la comisión de un hecho. Es evidente que se considera de máxima urgencia en el tiempo, los casos que tienen comprometida la vida, libertad de personas, seguridad del estado, cuyo riesgo es de nivel 1, o inminente. Una vez cumplidos los dos aspectos anteriores se procede a realizar la apertura ante la F.G.N.

Una vez se han cumplido los procedimientos previos, con la orden de la Fiscalía se procede a diligenciar los formatos correspondientes donde se registra el número de la resolución emitida por el Fiscal, cumplido este paso se da trámite ante la coordinación del sistema esperanza, dándose inicio al monitoreo de la línea.

3.2.2. Respecto de la documentación.

Se deben gestionar y custodiar los siguientes archivos:

- Archivo formato No. 002
- Archivo de documentación soporte de interceptación de cada objetivo.
- Archivo de planilla del Sistema esperanza.
- Archivo de comunicaciones entre el Sistema esperanza y la Sala.
- Registro y control de entrega de evidencias en medio magnético, de acuerdo con el procedimiento del Manuel de cadena de custodia.
- Registro de novedades técnicas del sistema de la sala.
- Registro de consultas por cell id, donde se indique: fecha, solicitante, objetivo, celda consultada, resultado, firma administrador del sistema y firma solicitante.

3.2.3. Seguridad de los Funcionarios

- Los funcionarios deben tener funciones de Policía Judicial.
- Debe ser personal con nivel de confianza demostrado.
- La antigüedad (Tiempo mínimo de permanencia en la institución) exigida para los cargos es: Jefe de Grupo cinco (5) años, Jefe de Sala tres (3) años, analista un (1) año, Administrador del Sistema un (1) año.
- Previamente a la asignación de los funcionarios al grupo de trabajo debe superar: Estudio de confiabilidad, acta de reserva o confidencialidad y de anticorrupción y prueba de Polígrafo.
- El tiempo mínimo de permanencia es de cinco (5) años, en el cargo o Sala de Interceptación.

3.2.4. Otros Procedimientos

4.2.4.1 Cancelación de las órdenes de interceptación

Se procede a cancelar las órdenes cuando se presenten los siguientes eventos:

- Si el resultado obtenido de las interceptaciones al término de 30 días es calificado como insatisfactorio, en consecuencia el fiscal de conocimiento enterado de esto definirá la situación mediante orden.

- Si los resultados de la interceptación, no obstante el corto tiempo transcurrido, son satisfactorios y suficientes para tomar decisiones en la investigación, de acuerdo a lo valorado por el Fiscal respectivo.

- Cuando producida la prórroga de una interceptación dada la subsistencia de los motivos fundados que la originaron, se alcance el límite máximo previsto en la ley, situación que deberá informar al despacho del conocimiento el coordinador de la respectiva sala.

- Cuando se vence el tiempo previsto, sin que se haya interpuesto prórroga.

3.2.5. Actividades finales

Una vez realizado el proceso de interceptación como se ha detallado arriba, el analista entre otras realiza las siguientes acciones:

- **Interpretación de la información:** Se materializa mediante un informe detallado de los hechos utilizando diagramas de flujo, de conexiones, bosquejos, relación de nombres con su perfil y acciones y oficios, en general elabora el entorno en el que se mueve el objetivo. De acuerdo con consultas hechas, algunos analistas señalan que en toda interceptación siempre aparecen o relacionan otros casos, algunas veces ha sucedido que el objetivo inicial de la investigación no se logra y en cambio aparece otro caso de mayor impacto, es decir nace una nueva investigación, así se han dado casos de alto impacto, con la captura de delincuentes altamente peligrosos. (No se indican los casos por reserva de la información).

- El informe debe estar sujeto al procedimiento señalado en el Manual de Policía Judicial.

- La información (grabación digital), se almacena en un medio magnético, el cual consiste en CD o DVD, se etiqueta con el número del proceso y entre en cadena de custodia, luego se solicita audiencia para el control de legalidad, entonces entra al almacén de evidencias de la Fiscalía.

- Al respecto el Manual de Procedimientos de las salas establece: "…Todo informe que salga de la sala de interceptaciones acompañado de casete, CD o DVD donde estén grabadas las conversaciones realizadas a través del abonado y que vayan con destino al fiscal de conocimiento del caso deberán ser embaladas, rotuladas y acompañadas del formato de cadena de custodia siempre y cuando se cuente con estos implementos.

- Las comunicaciones telefónicas y de recuperación de información dejada al navegar por internet[45] deben seguir los lineamientos establecidos en el procedimiento de “manejo de la información”.

- Antes de proceder a realizar la interceptación de comunicaciones telefónicas o de recuperación de la información dejada al navegar por internet es deber de los servidores de Policía Judicial asignados observar las condiciones establecidas en el Código de procedimiento Penal y Manual único de Policía Judicial.

3.3. Tecnologías de conexión física para Interceptación telefónica

- En cuanto a la tecnología para interceptar correos electrónicos:

  En una de las declaraciones que se recibieron por parte de la Fiscalía general de la nación, se evidencia el uso de estrategias para obtener información clave, al mismo tiempo se demuestra que no obstante se cuente con tecnologías de última generación, siempre la habilidad de las personas con experticia, pueden hacer uso de estrategias no tan sofisticadas, como “mensajes engañosos”, que cautivan e inducen a las personas a suministrar información importante. Como se muestra a continuación.

  "...no conozco sobre esos temas, porque mi única labor era la de análisis de la información de inteligencia obtenida y mediador para la consecución de nueva información de acuerdo con instrucciones recibidas en reuniones con el doctor NARVAEZ y el doctor NOGUERA. Voy a ser sincero, a mí una vez me comentaron, no recuerdo quien, que estas informaciones de correos electrónicos se lograban interceptar mediante un programa obtenido por internet que lanzaba un "anzuelo" para que el objetivo al responder generara la clave de ingreso para el correo electrónico, eso es lo que tengo entendido que se presentó en estos

[45] Consiste en capturar a través de medios técnicos, información útil para la investigación, transmitida por el indiciado o imputado, al navegar por Internet o similares. El Fiscal expide la respectiva orden cuando tiene motivos razonables y fundados de la existencia de información valiosa para la investigación.
Solicitar al fiscal del caso la orden para aprehender los equipos, medios magnéticos y de almacenamiento físico, para que expertos en informática forense descubran, recojan, recuperen, analicen y custodien la información
La incautación de estos elementos, se limita al tiempo necesario para la captura de la información contenida en los mismos y luego por orden del fiscal se devuelven a su propietario o tenedor.
En lo pertinente, según la naturaleza del acto se aplican analógicamente los criterios establecidos para registros y allanamientos. (4)

casos. Presumo que esto se inició desde el momento en que se creó el G3 para satisfacer las necesidades del grupo..."[46] [28].

- En relación con los equipos de interceptaciones:

"...los equipos para interceptaciones telefónicas están a cargo o en la sala de policía judicial que hace parte de la dirección general operativa, pero no sé cuántos equipos ni el tipo de tecnología especifico de los mismos, al parecer había una capacidad de equipos para escaneo del espectro electromagnético de ubicación celular de la tecnología anterior a GMty de los que se utilizan en áreas rurales, para frecuencia corta y amplia..."

3.3.1. Sistema Esperanza

Este "Proyecto", nace en la década del 2000, cuando se reúnen funcionarios de la Fiscalía General de la Nación y miembros de la DEA. En el año 2004 se consolida como "Proyecto esperanza, legalizándose en el año 2005, mediante el Acuerdo 038 de 2005, como un sistema de interceptación, interinstitucional entre la Fiscalía (entidad a la cabeza del sistema), Policía y DAS.

Capacidad de líneas:

Agosto 24 de 2010.

Capacidad instalada: 6270 líneas, simultáneas, en todo el país;

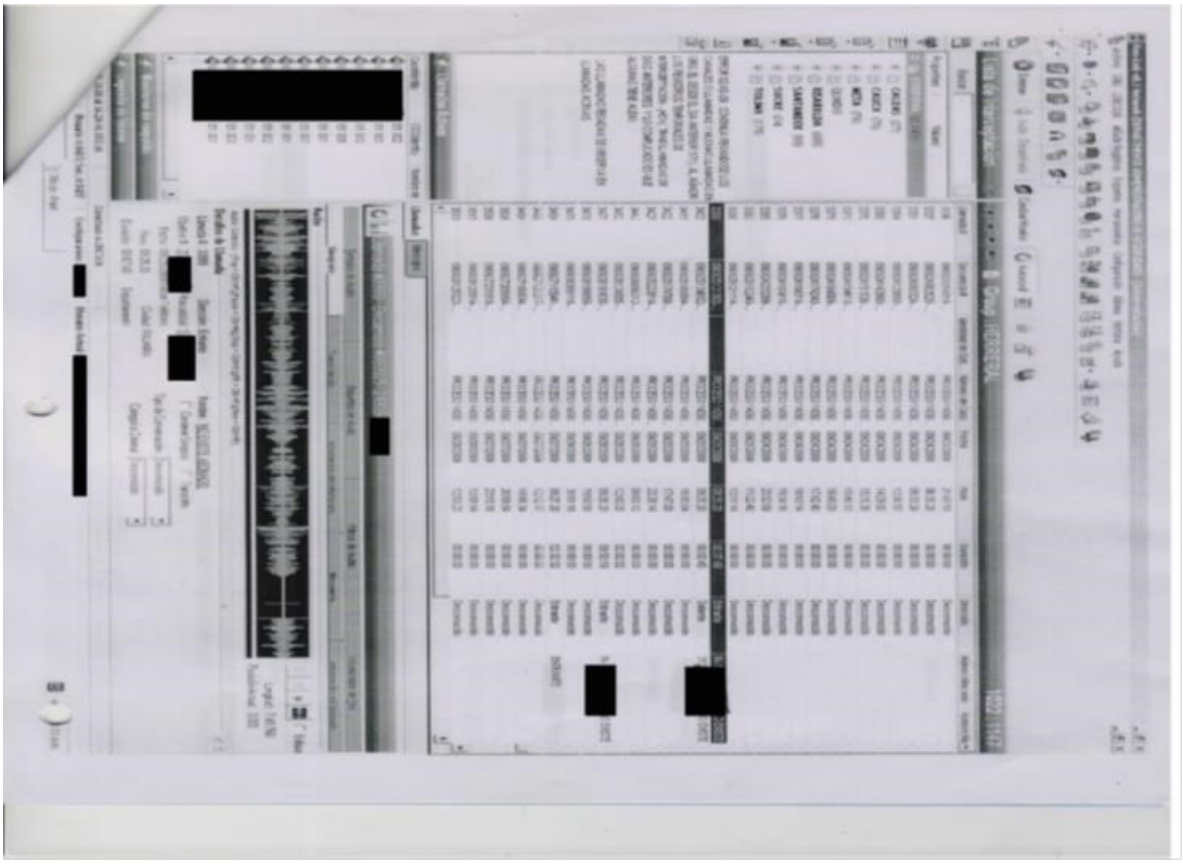
Servicios: Telefonía móvil,

No tiene: Interceptación de mensaje de voz, no se puede interceptar Black berry.[47]

La siguiente figura muestra la interfaz de consulta que provee el software proporcionado por la empresa estadounidense Pen-Link, el cual entre otras funciones permite ver información de la llamada en tiempo real de un objetivo específico.

[46] Fuente: http://www.derechos.org/nizkor/colombia/doc/das299.html#259
[47] Fuente: Acta 06 del 24/08/2010Pág. 28 – párrafo 1

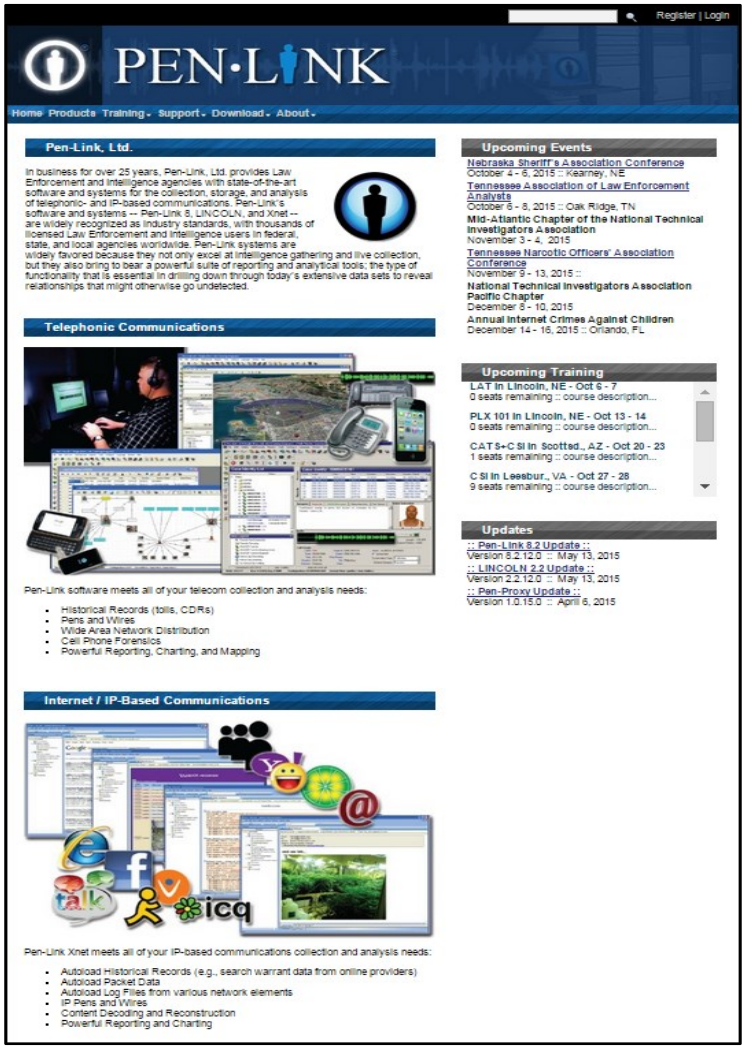
Figura 3-6: Aplicativo Sistema Esperanza [29]



3.3.1.1. Penlink

La página web de esta compañía, indica que tiene más de 25 años en el mercado, sus productos; aplicaciones de última generación para recolección, almacenamiento y análisis de sistemas de comunicaciones telefónicos. Sus productos están orientados principalmente a satisfacer las necesidades de entidades de Inteligencia de los gobiernos del Mundo. Como se observa, la compañía, tiene, pública su información en la web, indicando el objetivo principal de su negocio. En la siguiente figura se puede ver la presentación de la web de este proveedor.

Figura 3-7: Página de inicio de la compañía Pen-link [30]

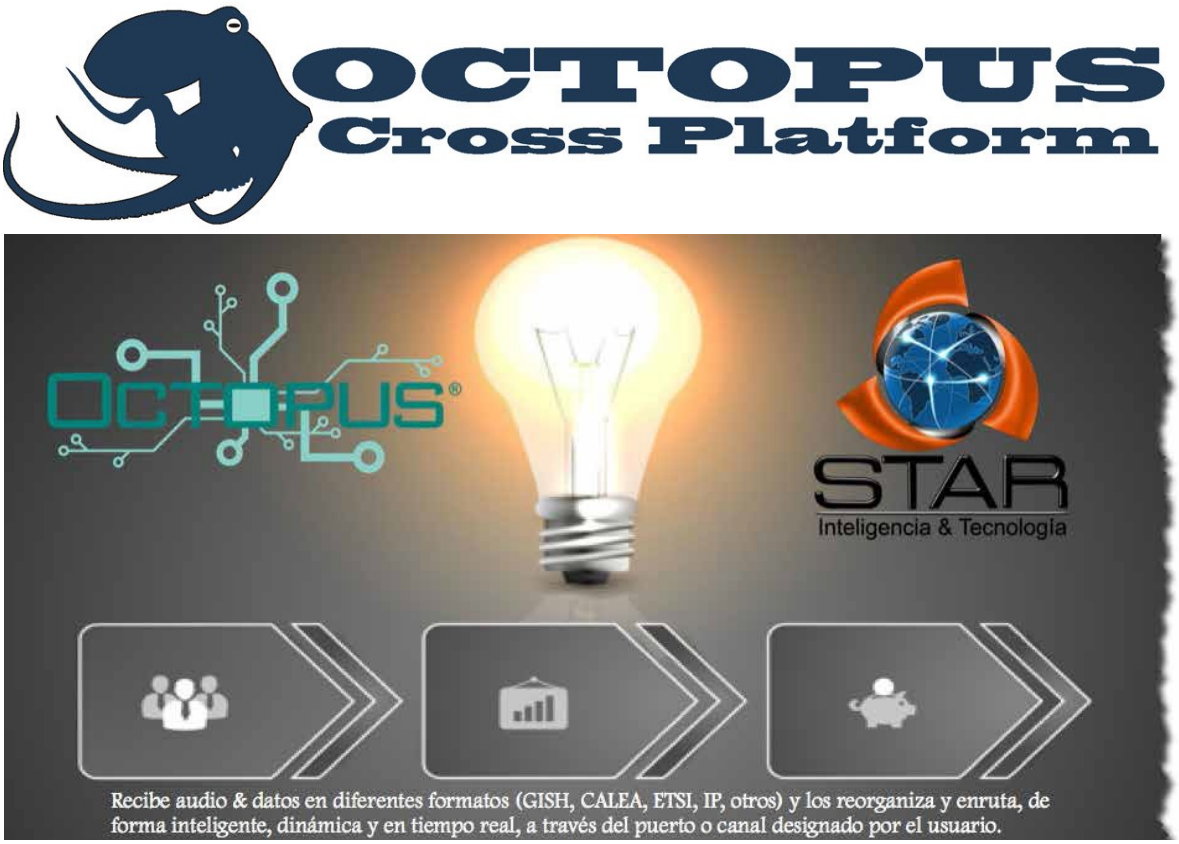


El proyecto esperanza, fue implementado por la compañía **STAR Inteligencia y tecnología,** Compañía Colombiana, que además es un proveedor exclusivo de productos de empresas británicas y estadounidenses para el sistema esperanza.

3.3.1.2. Octopus

Es una plataforma de interceptación suministrada por la compañía STAR, consiste en un switch de interconexión, que permite la conmutación de señales de diferentes protocolos; GSM, IP, así como protocolos de interceptación legal ETSI y CALEA, este es un sistema centralizado.

Figura 3-8: Presentación Suit de interceptación Octopus [29]



3.3.1.3. Proceso de interceptación en el sistema esperanza.

1. Solicitud formal por parte del analista de información ante funcionario de la Fiscalía para intervenir una línea o líneas específicas.
2. Justificar debidamente la solicitud de interceptación
3. El Funcionario responsable de la FGN, autoriza y determina el direccionamiento que debe tener la línea “intervenida”, a través del sistema Esperanza, y la sala específica en la cual se realiza la operación de escucha (grabación) de la línea.

En el año 2012, el sistema esperanza, disponía de unas 20 salas distribuidas en el País, de las cuales al menos 6 tenían apoyo financiero y técnico de la DEA. (Las salas se identifican por colores), como se indica en la siguiente figura.

Figura 3-9: Identificación de las salas de interceptación “Sistema esperanza” [29]

3.3.2. Sistema PUMA – Proyecto Ciberdefensa del País.

Sus instalaciones están ubicadas en un edificio ubicado en la carrea 63 # 19 – 04. Localidad de Puente Aranda (centro neuronal del Sistema PUMA)

Consiste en un sistema de interceptación más avanzado del sistema esperanza, y nace para suplir las debilidades y limitación de este sistema. Su operación inicia en año 2007 con ocho (08) salas:

a) Medellín
b) Barranquilla
c) Bucaramanga
d) Cúcuta
e) Pereira
f) Villavicencio
g) Neiva
h) Cali.

Siendo Operadas por Funcionarios de la Policía Nacional; Dijin, grupos Gaula y Sijin (Seccionales de Policía Judicial descentralizadas en los departamentos de Policía).

El sistema PUMA (Plataforma Única de Monitoreo y Análisis) está basado en tecnologías mucho más potentes e invasivas que las de Esperanza. Este sistema consiste en un switch en el que es necesario que un agente de la Fiscalía solicite a distancia al proveedor de servicios que le envíe información de una determinada línea intervenida. Sin esta solicitud, que se presenta en formato electrónico sobre la base de la aprobación de una solicitud por escrito de interceptación, no puede efectuarse la interceptación.

Figura 3-10: Instalaciones del Sistema PUMA [29]

Fuente: http://denotelopuedocreer.com.

PUMA, consiste en una plataforma tecnológica que permite interceptar y almacenar potencialmente todas las comunicaciones transmitas por los cables de alto volumen que componen la troncal de la que todos los colombianos dependen para hablar entre ellos y enviarse mensajes. No tiene la limitación del número de analistas disponibles para "encargar" a los proveedores de servicios que envíen información ni de los cupos de interceptación por proveedor. La tecnología de PUMA sólo está limitada por la capacidad de almacenaje de los servidores de su centro de monitoreo y la capacidad de las sondas colocadas en los cables de la troncal.

PUMA está vinculado directamente a la infraestructura de red de los proveedores de servicios, por medio de una sondas que direccionan directamente todos los datos al

centro de monitoreo de las autoridades policiales, sin necesidad de que lo facilite de nuevo el proveedor de servicios. En la actualidad, PUMA puede interceptar, almacenar y analizar cantidades masivas de tráfico telefónico, y está previsto que crezca y pueda también interceptar el tráfico de Internet..."[48]. En la siguiente tabla se detallan las salas del sistema PUMA, en el año 2010.

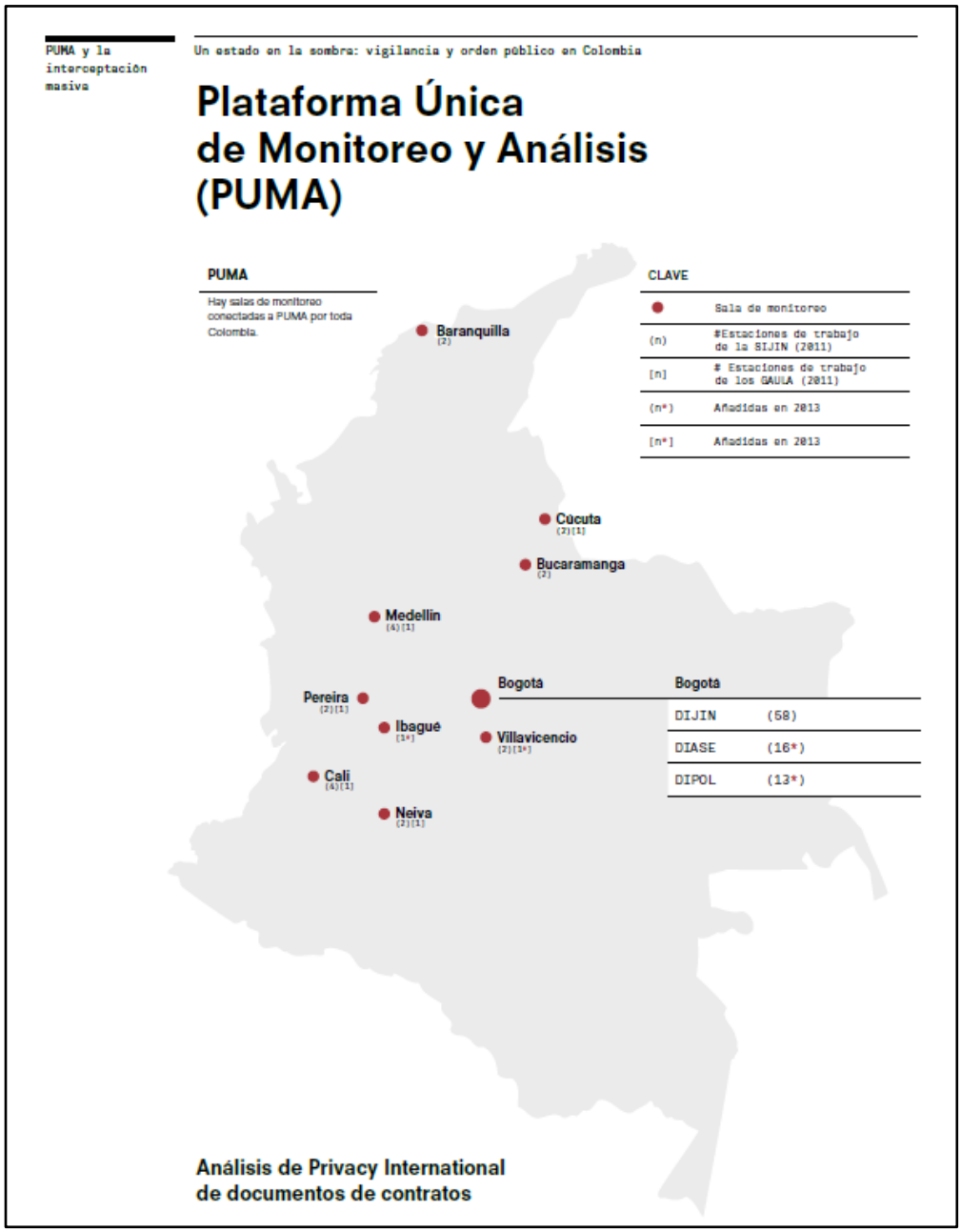
Tabla 3-1: Salas del Sistema PUMA

CIUDAD	UNIDAD	ESTACIONES DE TRABAJO	UBICACIÓN
Neiva	Gaula Huila	1	Calle 21 # 12 – 50 Tenerife
	SIJIN Neiva	2	
Cúcuta	GAULA Norte de Santander	1	Av. 3 Demetrio Mendoza No. 21-189
	SIJIN Cúcuta	2	Av. 6 # -97 Corral de piedra
Pereira	GAULA Risaralda	1	Av. las Américas con calle 46 (Comando de Policía Pereira)
	SIJIN Risaralda	2	
Cali	GAULA Valle	1	Cra 52 # 2 - 00
	SIJIN Cali	4	Av. Simón Bolívar No. 5-42
Medellín	GAULA Antioquia	1	Cra 51 # 14 – 239 Barrio. Guayabal.
	SIJIN Medellín	4	Calle 72 # 64 – 70 Edificio Antonio Bolívar Betancourt
Villavicencio	SIJIN Villavicencio	2	Calle 17 # 37 F – 47 Brr. Marsella
Bucaramanga	SIJIN Bucaramanga	2	Calle 41 No. 12-48
Barranquilla	SIJIN Barranquilla	2	Cra 38 # 74 – 90 Carrefour Americano
AÑO 2013 (83 estaciones en el País)			
Bogotá	DIJIN	58	Calle 26 con Av. Cali (Barrio Modelia)

En los últimos años, los sistemas de interceptación han sido ampliados, con la disposición de más salas.

[48] Ibídem

Figura 3-11: Distribución salas de interceptación Sistema PUMA [29]



El Tipo de información objetivo de PUMA, es la de “Inteligencia”, la cual se diferencia de la información obtenida como cumplimiento dentro de un proceso judicial, y trata antes, en que como su nombre lo indica, es información de inteligencia, que no se tipifica en una evidencia judicial, tampoco sirve para demostrar un hecho punible. Por tal razón la información de inteligencia, sirve como guía o indicio para solicitar una investigación, pero no como prueba fehaciente. En sentido riguroso y desde el punto de vista judicial, se puede indicar que no sirve para “nada”. Este quizás ha sido uno de los factores que en

varias ocasiones, ya sea por desconocimiento de parte de algunos funcionarios, o extralimitación en el ejercicio de sus funciones, ha dado lugar a "interceptaciones ilegales" motivo de escándalos al interior del estado.

3.3.3. Tecnologías de espionaje masivo adquiridas en Colombia:

3.3.3.1. **Verint**.

Empresa Israely, empresa especializada en la creación de software para mejorar la atención al cliente, centros de monitoreo de comunicaciones, tecnologías de vigilancia en video y localización de productos.

El portafolio de Verint, ha sido vendido en India, Israel, Costa de Marfil, Holanda, Eslovenia y estados Unidos[49].

"..De acuerdo con el vicepresidente de ventas para América Latina y el Caribe de Verint, Diego Gómez, Colombia es un país estratégico dentro de la región, por ser "un mercado sólido, estable, y porque los empresarios colombianos son serios y están comprometidos con la mejora del servicio al cliente..."[50] [31]. Al cerrar 2013, Verint tuvo ingresos de US$907 millones, y espera terminar este 2014 recibiendo US$1.130 millones.

Para este proyecto, en el Año 2013, se realizó una Inversión de recursos por US 50000, los cuales fueron asignados al proyecto PUMA en enero de este año, con el fin de convertirlo en la primera plataforma de interceptación.

.."La Policía asignó la suma sin precedente de 50.000 millones de pesos (28 millones de dólares estadounidenses) al proyecto en enero de 2013.37 Más de la mitad de esta cantidad se destinó a "fortalecimiento tecnológico", es decir, al software y hardware básicos necesarios para convertir PUMA en un sistema completo de interceptación legal, capaz de recopilar datos y contenido de llamadas de voz, VoIP, tráfico de Internet y redes sociales en 12 de los proveedores de servicios de telecomunicaciones de Colombia – cuatro redes de datos móviles y voz (Claro, Tigo, Avantel y Movistar) y ocho proveedores de servicios de Internet (Une, Telefónica, Emcali, Metrotel, ETB, Telebucaramanga, Telmex y EPM)... [30]"[51]

3.3.4. Empresas que suministran tecnologías y productos de interceptación.

[49] http://denotelopuedocreer.com/gran-hermano-la-era-del-monitoreo-en-internet-ha-iniciado-en-colombia-2/. 24/11/2014
[50] http://www.larepublica.co/verint-systems-planea-poner-una-oficina-en-colombia, de junio 18 de 2014
[51] Shadow State: Surveillance, Law and Order in Colombia, Agosto de 2015

3.3.4.1. STAR Inteligencia y tecnología

Es una empresa constituida desde mayo de 2004, es además el proveedor exclusivo de varios productos de empresas británicas y estadounidenses que son también componentes importantes del sistema Esperanza.

Una información interesante es que durante los primeros dos (02) años de funcionamiento de esta empresa, se dedicó exclusivamente en la creación e implementación del sistema esperanza, esto indica que prácticamente fue el objetivo con el cual se creó.

Aquí resultan varios interrogantes:

- ✓ Se sabía de antemano (antes de crearse STAR), que se iba a implementar un sistema de interceptación telefónica, para lo cual no existían empresas en el país capaces de suministrar este tipo de tecnología?
- ✓ Tanta influencia tienen los dueños de STAR, que antes de crear la empresa ya tenían su cliente definido.
- ✓ Se creó STAR exclusivamente para implementar el sistema esperanza?. Entonces esta empresa tiene socios que toman decisiones dentro de la Fiscalía, sobre el tema de interceptación?

Tabla 3-2: Información general empresa Star

Concepto	**Datos empresa**
Nit	830139912
Razón Social	Star Inteligencia & Tecnología S.A
Sector	Comercio Al Por Mayor
Ciudad	Bogotá-D.C.
Dirección	Av. (Cl) 26 68 C-61 Of 3273
Director	Oscar Reyes

Se puede indicar que STAR, es la empresa que creo ESPERANZA, para ello utilizo diferentes tecnologías, de origen británico y estadounidenses, para entregar una plataforma a la medida del cliente DIPOL. Los productos comercializados por STAR, consisten en Software y Hardware de interceptación, aplicaciones para análisis de grandes volúmenes de información (big data) y cores de mando y control entre otros.

Entre los proveedores de STAR se encuentra Komcept Solutions limted, empresa dedicada al diseño de sistemas de seguridad mediante la grabación de Audio y video y la recolección de evidencias para la aplicación de la ley.

En la siguiente grafica se muestra la presentación del sitio web www.komcept.com, de esta empresa.

Figura 3-12: Presentación web de komcept.com [32]

Productos de la compañía:

Soluciones de grabación y reproducción de audio de alta fidelidad, con transmisión a través de las redes de sistemas de telecomunicaciones, voz y fax.

Las herramientas gráficas de procesamiento opcionales le proporcionan un arsenal completo de interceptación telefónica, mediante el uso de módulos individuales para escalar el sistema de acuerdo a sus necesidades y presupuesto, y construir el sistema en el transcurso del tiempo.

Komcept solutions también puede suministrarle una gama de sistemas de vigilancia por satélite, y proporcionarle equipos de monitoreo de sistemas de radio.

Komcept Solutions Ltd. Solamente le suministrará soluciones de monitoreo e interceptación telefónica a clientes de gobiernos y sus agentes.

Figura 3-13: Equipos de Komcept solutions [32]

La figura 3-13, muestra algunos elementos que de forma comercial, ofrece Komcept para equipar una sala de interceptación. Dentro de los equipos de Komcept solutions, hay un maletín equipado con 144 micrófonos con procesador digital, con capacidad para grabar en un radio de 30 metros y transmitir la información vía bluetooth y/o wiffi, a un analista fuera del área.

Una Característica de Star, consiste en ser el único distribuidor autorizado de productos de varias empresas internacionales, al tiempo que es de las pocas empresas colombianas que manufacturan sus propios materiales de interceptación con marca registrada.

Al mismo tiempo Star tiene una empresa; Expert Design Solutions, ubicada en Panamá, la cual tiene a cargo el mantenimiento de los equipos de Komcept Solutions, ubicados en allí, así como los de estados Unidos y el reino Unido.

Debido a las relaciones comerciales, de Star con la Fiscalía General de la Nación, se convirtió en una de las empresas casi predilectas en el suministro de sistemas de inteligencia del Sector defensa; (Ejército, Armada, Fuerza Aérea, y Policía, así como las embajadas Británica, Estadounidense y Mexicana.

3.3.4.2. Pen-Link

Empresa de origen estadounidense, que de acuerdo con la información de su página web: https://www.penlink.com/Home/tabid/37/Default.aspx [29], lleva unos 25 años en el mercado, ofreciendo soluciones a diferentes gobiernos en el mundo, y en general a entidades encargadas de ejercer la aplicación de las leyes. Las soluciones ofrecidas consisten en hardware y software, para la recolección, almacenamiento y análisis de todo tipo de información de sistemas telefónicos y comunicaciones basadas en IP. Indica que son miles los clientes que tiene en el sector de inteligencia, dado que su sistema le permite establecer relaciones de datos, que el ser humano podrá pasar inadvertido en torno a un hecho punible o caracterización de una conducta en un proceso de investigación.

Entre los productos destacados de Pen-Link, se encuentra Lincoln, que consiste en una plataforma para servidores, la cual se gestiona mediante el **Software Pen-Link 8**,

a) **Pen-Link 8** [29]. Consiste en una suite de aplicaciones, para el análisis de la información captada de los sistemas de telecomunicaciones (Tráfico telefónico, como de datos baso en IP). Esta versión en particular se indica por parte de Pen-Link, es más amigable con el usuario y compatible con la mayoría de protocolos de comunicaciones, al mismo tiempo le permite realizar informes en tiempo real, también se dice que prácticamente la potencialidad y capacidades del sistema se hacen caso infinitas, en el uso de herramientas para el análisis de la información de voz y datos[52].

b) **Lincoln. "**Proporciona una solución de sistema completo para cualquier enfoque CALEA o basado en instalaciones basadas en redes de área local para la vigilancia electrónica. El sistema incluye hardware, software, enfocado a satisfacer las necesidades de interceptación de comunicaciones", este sistema está fundamentado en el modelo Cliente/servidor. El Software consiste en un servidor con un poderoso Software de gestión y administración, con interfaces para estaciones de trabajo, desde las cuales se realiza el análisis de información, como se indicó antes, esta plataforma se gestiona mediante Pen-Link 8.

El servidor LINCOLN está equipado con el hardware necesario para terminar las conexiones físicas de la interfaz de correo, en la compañía. La plataforma actúa como un nodo pasivo en las redes de los operadores de telecomunicaciones, de esta forma se

[52] http://www.penlink.com/Products/tabid/54/Default.aspx

tiene en tiempo real el análisis de las líneas, y datos interceptados de las cuentas objetivo.[53]

La participación de Pen-Link en el proyecto esperanza, consistió entre otros en suministrar la interfaz que les permite a los funcionarios de inteligencia gestionar y analizar el contenido de los datos de cada una de las líneas telefónicas interceptadas.

Cabe resaltar que Pen-Link, es uno de las compañías proveedoras de tecnología de inteligencia, preferidas de la Administración para el control de Drogas; DEA, (Drugs Enforcement Agency, DEA), Al mismo tiempo esta empresa le ha suministrado a la embajada de Estados Unidos en Colombia, el Software que se utiliza en la sala de interceptación que se tiene allí instalada, bajo la administración de funcionarios americanos.[54]

3.3.4.3. Verint Systems.

Esta empresa, tienen varias filiales en diferentes países; Verint Systems Ltda., empresa israelí es socia de Verint Systems Inc. De los Estados unidos.

La Compañía Israelí ha vendido a Colombia gran cantidad de tecnología de vigilancia.

El hecho más importante de esta compañía, consiste en que fue la empresa que le suministró a la Policías Nacional - DIJIN, el sistema PUMA.

El sistema PUMA: Es considerado el sistema de interceptación más robusto que se tenga en Colombia, sin embargo este no reemplaza a los demás sistemas, sino que se complementan. De esta forma se pueden compartir información entre sí, permitiendo disponer de una infraestructura muy robusta para los procesos de interceptación y monitoreo.

PUMA, es capaz de recopilar doto tipo de información que transite a través de una troncal, para ello utiliza una “sonda”, mediante la cual se interconecta al “CORE” del proveedor de comunicaciones, capturando todo tipo de información, así no se requiere de personal que realice manipulación o gestión de la red, actuando en forma pasiva y si realizar la más mínima interferencia en la operación normal de la red de telecomunicaciones del operador.

Una vez se realizó la ampliación del sistema, este tiene la capacidad de interceptar las redes de comunicaciones 4G.

---

[53] Ibídem

[54] Demanda y oferta: la industria de la vigilancia al descubierto, informe especial-julio de 2015. Se encuentra en: https://www.privacyinternational.org/sites/default/files/DemandSupply_Espanol.pdf

3.3.4.4. Sistema SIGD (Sistema Integral de Grabación Digital)

Este sistema fue adquirido por la POLICIA NACIONAL - DIPOL, Dirección encargada de la Inteligencia y contrainteligencia de la Policía, la plataforma adquirida, Utiliza la misma tecnología del sistema PUMA.

"Con 910 millones de dólares estadounidenses de ingresos en 2014,45 Verint Systems forma parte del pequeño grupo de líderes mundiales de la tecnología para centros de monitoreo. En su catálogo de material de comunicaciones y ciberinteligencia, vende soluciones de ciberseguridad, tecnología de rastreo móvil, dispositivos de interceptación táctica que sirven para interceptar llamadas de móviles y herramientas analíticas de código abierto. Por ejemplo, su sistema SkyLock se presenta como una herramienta capaz de rastrear la ubicación de un teléfono móvil en cualquier lugar del mundo.46 Con la vista puesta en los TSP y los organismos de inteligencia y encargados de hacer cumplir la ley, Verint Systems vende centros de monitoreo que "posibilitan la interceptación, monitoreo y análisis de comunicaciones específicas y masivas prácticamente en cualquier red" y que, según el sitio web de la empresa, se utilizan en más de 75 países"[55].

Entre los Países a los cuales Verint Systems, les provee tecnologías de inteligencia se encuentran: Kazajistán y Uzbekistán, desafortunadamente en estos países sus gobiernos realizan una represión política y vigilancia tecnológica de comunicaciones sobre toda la sociedad.

Una característica de este sistema es que no está sujeto a vigilancia selectiva, por ser un sistema táctico puede en forma dinámica seleccionar nuevos objetivos. La capacidad de procesamiento de tráfico es de 2 Mbps (un E1) o más si se quiere.

De acuerdo con información de la Compañía Verint Systems, señala que sus sistemas de monitoreo corresponden a dos áreas Funcionales:

a) Back-end o pate trasera conformada por el centro de monitoreo, en el cual los analistas solicitan y reciben datos.
b) Front-end (parte delantera) instalada en la misma red de telecomunicaciones, encargada de interceptar los datos antes de enviarlos al centro de monitoreo[56].

Con sus tecnologías de alta capacidad, la empresa durante la última década, ha sido pionera en el desarrollo de un sistema de alta capacidad de interceptación masiva en el país.

[55] Demanda y oferta: La industria de la vigilancia al descubierto
[56] Ibídem

3.3.4.5. Curacao.

Empresa Colombiana, representante exclusivo de Verint Systems en Colombia. Fue la encargada de proveerle una sonda táctica al DAS, lo particular de esta interface es que era dinámica y se podía operar en cualquier parte del país.

Como hecho transcendental, durante el proceso de contratación de la modernización del sistema PUMA, se presentó una rivalidad entre las firmas: Curacao e Eagle Commercial, y dado que son los dos representantes de dos de las más afamadas y poderosas empresas de tecnología de inteligencia: Nice Systems y Verint Systems, el hecho debió realizar un proceso, a nivel interno de la Policía, debido a que la empresa Curacao exigía se le asignara el contrato de mantenimiento del sistema PUMA por contratación Directa, tras el hecho de ser representante exclusivo de Verint Systems. Esta situación creo rivalidad debido a que el contrato por más de 35 millones de Dólares le fue asignado a la Empresa Eagle Commercial en unión con Nice Systems [33].[57]

3.3.4.6. NICE Systems:

Empresa Israelí, fue fundada en 1986 por miembros del Ejército Israelí, su sede se encuentra en Ra'anana, Israel, suministra soluciones tecnológicas para contact center, protección y sectores de seguridad pública, y la prevención de delitos financieros. De acuerdo con la información de su página web, cuenta con más de 25000 clientes y realiza operaciones comerciales en más de 150 países. En América Latina tiene oficinas en Sao Paulo y Ciudad de México[58].

Tabla 3-3: Información general Nice Systems [34]

Concepto	**Datos empresa**
Razón Social	NICE Systems Ltd.
Sector	Comercio de tecnologías
Dirección	22 Zarhin Street, P.O. Box 690, Ra'anana, Israel
Teléfono	972-9-7753777
Email	ir@nice.com
Sitio web	http://www.nice.com/ [34]

[57] http://caracol.com.co/radio/2014/04/25/judicial/1398407940_194095.html
[58] http://www.nice.com/

El papel de Nice sistemas, consistió en la ampliación del sistema PUMA, la cual consistía en ampliar la capacidad de interceptación a 20000 abonados simultáneos, y la posibilidad de ampliar a 100000 interceptaciones. Además el monitoreo de trafico IP. Para la operación del sistema se dispone de 70 estaciones de trabajo en todo el territorio colombiano.

La infraestructura para la interceptación del tráfico consistía en 8 sondas "NiceTrack IP", conectadas directamente a las red de los proveedores de servicios, y con ellas se extrae y analiza todo el tráfico que circule por allí.

Para su operación Nice, cuenta con tres áreas o líneas de tecnología:

a) **Nice Enterprice,** Línea especializada en centros de llamadas, plataformas para el análisis de Big data y análisis de voz.

b) **Nice Actimize:** dedicada al sector financiero, donde cuentas con herramientas para prevenir el blanqueo de dinero entre otras.

c) **Nice Security:** Suministra servicios de vigilancia electrónica; sistemas de grabación y análisis de video, interceptación de telefonía vía satélite con capacidad para rastrear y localizar un dispositivo en cualquier lugar. También cuenta con herramientas tecnológicas para el análisis de patrones, con las que se puede identificar una conducta delictiva. (Patter Analyzer)[59]

3.3.4.7. **Eagle Commercial S.A**

De acuerdo con la información de su página web, es una empresa Colombiana, dedicada al sector de las telecomunicaciones e ingeniería electrónica, especializada en asesoría y suministro de herramientas tecnologías a las entidades de seguridad del estado, para los cuales desarrolla proyectos a la medida.

Entre sus clientes menciona:

- Ministerio de defensa Nacional
- Policía Nacional
- DIPOL
- INPEC
- Ejército Nacional
- Fiscalía general de la Nación

[59] http://www.nice.com/intelligence-lea/pattern-analyzer

Además de ser representante en Colombia de Nice Systems, también lo es de American Harris Corporation y Taser International Inc.

3.4. Tecnologías de Interceptación Táctica

La interceptación táctica, está orientada a escuchar, grabar, almacenar y/o interferir comunicaciones, inalámbricas, también a través de un dispositivo específico. Consisten en equipo móviles que se pueden utilizar en diferentes partes como medio estratégico y táctico, esto indica que para su operación no necesitan estar conectados a una red físicamente.

En Colombia, se han adquirido tecnologías como los **IMSI catchers** (International Mobile Subscriber Identity) y herramientas de intrusión. Los primeros consisten en un dispositivo que actúa entre el dispositivo del usuario y el sistema de transmisión del proveedor de servicio, a este método se le conoce como **"hombre en el medio",** para ello el IMSI catchers emite una señal más fuerte que el operador, engañando al equipo móvil, entonces hace que este se conecte al sistema de interceptación, el cual a su vez pasa la llamada al operador, así puede en tiempo real gravar una conversación y transmitirla a un destinario específico, o en su defecto grabar datos para su posterior retransmisión. El IMSI cathchers, en este caso para la identificación del dispositivo lo hace mediante el identificador internacional del equipo móvil.

3.4.1. Empresas y tecnologías tácticas

Con el fin de evitar un extensa literatura acerca de las empresas que proveen tecnologías de interceptación táctica, toda vez que en la mayoría de casos se trata de las mismas empresas estudiadas antes, se realizó una revisión de las tecnologías que se han utilizado en Colombia y en otros países, resaltando los datos más importantes y consolidando esta información en la siguiente tabla.

Tabla 3-4: Tecnologías de interceptación táctica

No.	Empresa	Tecnología	Descripción	Origen de la empresa	O.B.S
1	Spectra Group	IMSI catchers o stingrays	Suministro su sistema "Laguna" a DIPOL (2005)	Reino Unido	
2	Smith Myers	Bulldog	Es un IMSI catchers	Reino Unido	Adquirido por el DAS en 2010, (US 250000) Fiscalía - DIJIN
		Nesie	Es un IMSI catchers		Adquirido por el DAS en 2010, (US 320000)
3	AcceeData		Proveía Software al DAS para análisis forense	Estados Unidos	
4	Hacking Team	Remote Control System (RCS)	Se destaca por el desarrollo de malware. (permite controlar a distancia determinados dispositivos) Infectando el dispositivo del objetivo, la suite RCS puede recopilar datos de él, activar y desactivar a distancia la webcam y el micrófono y copiar archivos y contraseñas tecleadas. Participo en PUMA.	Italia	Una vez instalado, el malware ataca y explota la memoria y el sistema operativo del dispositivo, permitiendo que un analista controle éste a distancia. La Policía su principal cliente. La DEA, Embajada de EEUU en Colombia.
5		IMSI catchers o stingrays	Sistema que simula un repetidor, torre o unto de acceso de la empresa de Comunicaciones	El número IMEI pero el número IMSI cambie a menudo	

No.	Empresa	Tecnología	descripción	Origen de la empresa	O.B.S
6	Maicrotel Ltda.		Sirvió de intermediario para el Suministro su sistema “Laguna” a DIPOL (2005)	Colombia	
7	Empresa de Telecomunicaciones Exfor	IMSI catcher NetHawk F10	Exporto esta tecnología a la Policía de Colombia, (DIPOL)	Canadá	
8	STAR	GSM Tracking System	Tecnología fabricada por Nokia (de origen Finlandes)	Colombia	Destino Escuela de Inteligencia del Ejercito
9	TAMCE	IMSI/IMEI catcher 3G	Tecnología que usa sistema basado en GPS	México	
10	Curacao	Software Forensic Toolkit 3.0(FTK)	Permite recuperar información de discos duros.	Colombia	DAS – DIPOL-DIJIN
11	Internet Solutions Ltda.	conjunto de programas de informática forense	Este software lo produce la Compañía Access Data	(EEUU)	DIPOL- DIJIN

4. Desarrollo de una propuesta regulatoria y técnica sobre la interceptación telefónica en Colombia

A través del documento se ha estudiado y analizado las herramientas de interceptación telefónica, tanto en el área regulatoria como técnica. A continuación se presenta una propuesta en lo regulatorio y lo técnico, la cual resulta del estudio presentado aquí.

4.1. Área regulatoria

Durante el estudio realizado desde el primer semestre del año 2010, en conjunto con una de las entidades encargadas de realizar labores de seguridad, se desarrolló un trabajo con el objeto de presentar un propuesta en materia de normatizar el proceso de interceptación telefónica, en lo referente a la función que cumple y deben cumplir los Operadores de telecomunicaciones, decretar unas obligaciones y responsabilidades de ambas partes; La entidad del estado y los operadores, toda vez que para la época el proceso de interceptación carecía de cualquier norma, excepto lo establecido en la constitución Política de Colombia los artículos 15 y 250 y el código de procedimiento penal en su capítulo séptimo.

NOTA: Se omite la incorporación de la propuesta por tratarse de información confidencial y reservada. (Documento de siete (07) páginas).

4.2. Resultados obtenidos de la propuesta.

Como se indicó durante el estudio realizado, desde diferentes sectores de la sociedad se solicitaba la regulación del proceso de interceptación, a continuación se describen los alcances y logros de la propuesta presentada aquí:

5.1.1. Ley 1453 del 24 de junio de 2011

Mediante el artículo 52. **Interceptación de Comunicaciones,** se modificó el artículo 235 de la ley 904.

- ✓ Primer logro de la propuesta: reforma de la ley 904; articulo 235 y

Texto original de la Ley 906 de 2004[60] [35]**:**

ARTÍCULO 235. El fiscal podrá ordenar, con el único objeto de buscar elementos materiales probatorios y evidencia física, que se intercepten mediante grabaciones magnetofónicas o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación. En este sentido, las entidades encargadas de la operación técnica de la respectiva interceptación tienen la obligación de realizarla inmediatamente después de la notificación de la orden.

En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.

Por ningún motivo se podrán interceptar las comunicaciones del defensor.

La orden tendrá una vigencia máxima de tres (3) meses, pero podrá prorrogarse hasta por otro tanto si, a juicio del fiscal, subsisten los motivos fundados que la originaron.

Texto modificado por la Ley 1142 de 2007:

ARTÍCULO 235. INTERCEPTACIÓN DE COMUNICACIONES TELEFÓNICAS Y SIMILARES. El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados o indiciados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación. En este sentido, las entidades encargadas de la operación técnica de la respectiva interceptación tienen la obligación de realizarla inmediatamente después de la notificación de la orden.

[60] Fuente: http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004_pr005.html

En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.

Por ningún motivo se podrán interceptar las comunicaciones del defensor.

<Aparte subrayado CONDICIONALMENTE exequible> La orden tendrá una vigencia máxima de tres (3) meses, pero podrá prorrogarse hasta por otro tanto si, a juicio del fiscal, subsisten los motivos fundados que la originaron.

La modificación propuesta fue:

ARTÍCULO 19. El artículo 235 del Código de Procedimiento Penal quedará así:
ARTICULO 235. INTERCEPTACION DE COMUNICACIONES. El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados o indiciados, que se intercepten mediante grabación magnetofónica, digital o similares, las comunicaciones telefónicas, radiotelefónicas, telegráficas, telemáticas, de valor agregado y/o de transmisión de datos o similares que utilicen sistemas informáticos y en general cualquier servicio de telecomunicaciones, cuya información tenga interés para los fines de la actuación. En este sentido, las entidades públicas o privadas encargadas de la operación técnica de la respectiva interceptación tienen la obligación de realizarla inmediatamente después de la notificación de la orden.
En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.
Por ningún motivo se podrán interceptar las comunicaciones del defensor.
La orden tendrá una vigencia máxima de tres (3) meses, pero podrá prorrogarse hasta por otro tanto sin que supere cuatro periodos consecutivos, si a juicio del fiscal, subsisten los motivos fundados que la originaron.

ARTÍCULO 235. INTERCEPTACIÓN DE COMUNICACIONES. <Artículo modificado por el artículo 52 de la Ley 1453 de 2011. El nuevo texto es el siguiente:>

El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación.

Jurisprudencia Vigencia
En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.

Por ningún motivo se podrán interceptar las comunicaciones del defensor.

La orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron.

La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías.

Texto original de la Ley 906 de 2004:
ARTÍCULO 236. RECUPERACIÓN DE INFORMACIÓN DEJADA AL NAVEGAR POR INTERNET U OTROS MEDIOS TECNOLÓGICOS QUE PRODUZCAN EFECTOS EQUIVALENTES. Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen.

En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos.

La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados.

ARTICULO 20. El artículo 236 del código de Procedimiento Penal quedará así:

ARTICULO 236. RECUPERACION DE INFORMACION. Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha utilizado dispositivos de almacenamiento digital o transmitido información útil para la investigación que se adelanta, durante su navegación por internet u otros medios tecnológicos que produzcan efectos equivalentes, podrá ordenar la preservación y aprehensión de los datos informáticos o sistemas informáticos y de comunicaciones, y demás medios de almacenamiento físico, para que investigadores en informática forense descubran, recojan, analicen y custodien la información que recuperen.

En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos sin tener en cuenta el horario. La preservación y aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información.
ARTÍCULO 236. RECUPERACIÓN DE INFORMACIÓN PRODUCTO DE LA TRANSMISIÓN DE DATOS A TRAVÉS DE LAS REDES DE COMUNICACIONES. <Artículo modificado por el artículo 53 de la Ley 1453 de 2011. El nuevo texto es el siguiente:> Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado. En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos. La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados, de ser el caso.

El segundo alcance de la regulación propuesta fue dar origen al Decreto 1704 [19] del 15 de Agosto de 2012. "Por medio del cual se reglamenta el artículo 52 de la Ley 1453 de 2011, se deroga el Decreto 075 de 2006 [25] y se dictan otras disposiciones".

Por otra parte del Análisis a la legislación nacional en materia de interceptación telefónica, se evidencia:

- ✓ Una falta de correspondencia entre las leyes nacionales y los tratados internacionales, por esta razón es imprescindible ajustar las normas, como la ley 1621 de 2013, al ordenamiento internacional en materia de derechos humanos, específicamente en cuanto a los tiempos de retención de la información de los usuarios vigilados.

- ✓ Se deben ajustar también las normas a las nuevas tecnologías, y permitir que estas normas sean dinámicas y se actualizar al tiempo que cambian o surgen nuevas herramientas tecnológicas. En el caso de las interceptaciones, la

tendencia mundial es el uso de la voz sobre IP, situación que debe redefinir y/o precisar el lenguaje en las normas.

- ✓ En materia de retención de información por parte de las empresas de telecomunicaciones, es vital definir en qué términos se hace esta retención de la información, que parámetros específicos se incluyen, los tiempos y si definitivamente el usuario tendrá o no derecho a conocer si es vigilado, si fue y desde cuándo, además si este puede controvertir y/o aclarar la información recolectada por los organismos de inteligencia, sopena de ser juzgado sin la garantía de un debido proceso.

- ✓ Queda demostrado en el estudio realizado, que hoy no es posible desarrollar procesos de seguimiento y lucha contra los delitos sin incluir la cooperación internacional, en consecuencia las tecnologías implementadas, son el producto de esta cooperación, en este sentido se debe proyectar y desarrollar normatividad internacional, específica que considera como un solo territorio las redes de datos a nivel internacional, es decir considerar leyes universales, que les permita a los países realizar acciones a nivel internacional a nivel de la redes. Para ello deben establecerse los mecanismos y normas de cooperación ajustadas al derecho de cada uno de los países, prevaleciendo los principios universales.

- ✓ Desarrollar un política entorno a la obligación que deben tener los operadores de comunicaciones en cuanto a la renovación, actualización y/o implementación de nuevas tecnologías, la cual se debe orientar para que cualquier operador ubicado en Colombia que preste servicios de telecomuniciones, cuando requiera modificar, modernizar, y/o actualizar la tecnología (hardware y software), con un tiempo no menor a (06) seis meses, debe informar al ministerio de las tics, Fiscalía general de la Nación y organismos de seguridad del estado entre otros, las características de las nuevas tecnologías y la forma en que estas pueden afectar la conectividad existe con estos organismos a través de la cual se realiza los procesos de vigilancia tecnológica. De la misma forma debe garantizar los puntos de acceso a sus bases de datos que se requieran para desempeñar en forma eficiente las labores de estos organismos.

4.3. Área Técnica

En este aspecto, con el fin de realizar una análisis serio a fin de determinar los factores que en materia tecnológica afectan el proceso de interceptación, y han dado lugar a la serie de hechos presentados en este trabajo, se hizo el estudio del proceso de “Interceptación telefónica”, para esto se realizó un análisis de riesgos a partir la norma Internacional ISO 31000 [36] “Gestión de Riesgos - Principios y Guías”, y la “Guía para la Administración del riesgo del departamento Administrativo de la Función Pública¨ [37]. De

la misma forma se incorporaron elementos de la norma ISO 27001 [38], "Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos".

A continuación se presenta el desarrollo de la Matriz de riesgos del proceso "Interceptación telefónica"

4.3.1. Matriz de riesgo del proceso: interceptación telefónica

Objetivo

Aplicar los elementos de seguridad que garanticen la integridad y la reserva de la información, durante las actividades de interceptación de la institución.

4.3.2. Contexto estratégico[61]:

Tabla 4-1: Factores Internos y externos del Riesgo [39]

Factores Internos	Factores externos
Infraestructura: ✓ Salas de interceptación inadecuadas ✓ Bases de datos vulnerables ✓ Servidores sin controles adecuados ✓ Canales de datos con el Operador de Telecomunicaciones sin protocolos definidos ✓ Operadores de Telecomunicaciones, con funcionarios corruptos, sin control que vendan la información de los usuarios. ✓ Equipos tácticos operados con fines fraudulentos	**Económicos** ✓ Sobredimensión de costos de los equipos
Personal ✓ Perfiles de funcionarios no adecuados ✓ Sin Capacitación ✓ Falta de Idoneidad para el manejo de la operación. ✓ Funcionarios corruptos ✓ Problemas de salud del personal que realiza el análisis de información.	**Medio ambientales** ✓ Emisiones de dióxido de carbono por parte de tecnologías de interceptación. ✓ Disposición inadecuada de la RAEES (Residuos de aparatos eléctricos y electrónicos), porque o existen gestores adecuados.

[61] "Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución". Fuente: Guía para la administración del riesgo del Departamento Administrativo de la Función Pública.

Factores Internos	Factores externos
Procesos ✓ Realizar interceptación sin orden de autoridad competente ✓ Sobrepasar los tiempos de la orden judicial. ✓ Dejar de realizar la interceptación, previa orden judicial.	**Políticos** ✓ Normatividad no adecuada conforme al alcance de la tecnología. ✓ Normatividad con vacíos legales ✓ Tráfico de influencias de altos cargos ✓ Congreso amaña la legislación con intereses particulares. ✓ No hay un procedimiento legal para la adquisición de tecnologías de interceptación.
Tecnología ✓ Uso inadecuado de las herramientas de interceptación con fines personales ✓ Herramientas de software incompatibles, que no sean escalables. ✓ Uso de tecnologías de interceptación ilegales. Equipos con conexión física y táctica. ✓ Uso de los equipos para escuchar mayor rango de líneas al autorizado legalmente. ✓	**Sociales** ✓ Persecución de determinados sectores sociales. ✓ Uso de la información con fines terroristas. ✓ Uso de la información de los usuarios con fines extorsivos. ✓ Violación de los derechos humanos.
	Tecnológicos ✓ Uso de tecnologías emergentes por los delincuentes ✓ Hackers ✓ Ingeniería social con fines delictivos ✓ Ausencia de controles de software malicioso en equipos vitales del sistema. ✓

El Primer paso consistió en definir los factores Internos y Externos que inciden el Proceso “Interceptación de comunicaciones telefónicas”. Hay que indicar que para este trabajo “la Matriz de riesgos, se conformó un Grupo de trabajo con expertos tanto en el análisis de riesgos como en el proceso de interceptación, que llevan en promedio unos 18 a 20 años en la entidad.

Tabla 4-2: Contexto Estratégico

Proceso: Interceptación de Comunicaciones telefónicas			
OBJETIVO: Aplicar los elementos de seguridad que garanticen la integridad y la reserva de la información, durante las actividades de interceptación de la institución.			
FACTORES EXTERNOS	**CAUSAS**	**FACTORES INTERNOS**	**CAUSAS**
Sobredimensión de costos de los equipos	- Corrupción - Empresas que sobredimensionan costos. - Existe el paradigma que todas las tecnologías de interceptación deben ser costosas. - Son tecnologías de punta	Salas de interceptación inadecuadas	- Infraestructura obsoleta - Corrupción - Falta de proyectos de desarrollo tecnológico.
Emisiones de dióxido de carbono por parte de tecnologías de interceptación.	- No cumplir con las normas de medio ambiente. -	Bases de datos vulnerables	- No se tienen implementadas políticas de seguridad de la información - Corrupción.
Disposición inadecuada de la RAEES (Residuos de aparatos eléctricos y electrónicos), porque no existen gestores adecuados.	- No hay gestores de RAAES autorizados	Servidores sin controles adecuados	- No inversión de controles técnicos. - No se tienen implementadas políticas de seguridad de la información
Normatividad no adecuada conforme al alcance de la tecnología.	- Intereses políticos - Trámite legal de las normas - Es más rápida la Evolución de la tecnologías	Canales de datos con el Operador de Telecomunicaciones sin protocolos definidos	- Falta de Políticas de seguridad. - Corrupción. - Operadores de Telecomunicaciones, con funcionarios corruptos, sin control que vendan la información de los usuarios.
Normatividad con vacíos legales	- Corrupción	Equipos tácticos operados con fines fraudulentos	- Falta de Políticas de seguridad. - Corrupción.

FACTORES EXTERNOS	CAUSAS	FACTORES INTERNOS	CAUSAS
Tráfico de influencias de altos cargos	- Intereses personales - Intereses de determinados grupos sociales.	Perfiles de funcionarios no adecuados	- Falta de un procedimiento de selección de personal adecuado - Sin Capacitación - Falta de Idoneidad para el manejo de la operación.
Congreso amaña la legislación con intereses particulares.	- Intereses personales - Intereses de determinados grupos sociales. - Corrupción	Funcionarios corruptos	- Falta de un procedimiento de selección de personal adecuado - Bajas remuneración de los funcionarios según su cargo. - Falta de ética profesional de los funcionarios
No hay un procedimiento legal (Controles) para la adquisición de tecnologías de interceptación.	- Debilidades normativas - No hay controles por parte del estado para la comercialización y adquisición de estas tecnologías.	Problemas de salud del personal que realiza el análisis de información.	- Equipos inadecuados - Falta de políticas de salud ocupacional
Persecución de determinados sectores sociales.	- Manejo de la información por parte de quienes tienen acceso a ella. - Venta de la información con fines ilegales.	Realizar interceptación sin orden de autoridad competente	- Inmediatez de los hechos - Corrupción - Desconocimiento del procedimiento - Extralimitación de las funciones asignadas.
Uso de la información con fines terroristas.	- Manejo de la información por parte de quienes tienen acceso a ella. - Venta de la información con fines ilegales.	Sobrepasar los tiempos de la orden judicial.	- Corrupción - Desconocimiento del procedimiento - Extralimitación de las funciones asignadas.
Uso de la información de los usuarios con fines extorsivos.	- Manejo de la información por parte de quienes tienen acceso a ella. - Venta de la información con fines ilegales. - Operadores de Telecomunicaciones, con funcionarios corruptos, sin control que vendan la información de los usuarios.	Dejar de realizar la interceptación, previa orden judicial.	- Corrupción - Desconocimiento del procedimiento - Extralimitación de las funciones asignadas.
Violación de los derechos humanos.	- Ejercicio del poder - Corrupción política - Debilidad del estado en decisiones judiciales - Normatividad débil	Uso inadecuado de las herramientas de interceptación con fines personales	- Corrupción - Extralimitación de las funciones asignadas. - Abuso de autoridad - Bajas remuneración de los funcionarios según su cargo.

FACTORES EXTERNOS	CAUSAS	FACTORES INTERNOS	CAUSAS
Uso de tecnologías emergentes por los delincuentes	No hay controles por parte del estado para la comercialización y adquisición de estas tecnologías.	Herramientas de software incompatibles, que no sean escalables	- Desconocimiento acerca de tecnologías de escala. - Asesorías inadecuadas - Intereses personales
Hackers	Herramientas de seguridad débiles. Corrupción de funcionarios de las organizaciones	Uso de tecnologías de interceptación ilegales. Equipos con conexión física y táctica.	- No hay controles por parte del - estado para la - comercialización y adquisición - de estas tecnologías. - Corrupción - Inmediatez
Ingeniería social con fines delictivos	Corrupción de funcionarios de las organizaciones No aplicar u observan las políticas de seguridad de la información	Uso de los equipos para escuchar mayor rango de líneas al autorizado legalmente	- Corrupción - Intereses personales - Extralimitación de las funciones asignadas.
Ausencia de controles de software malicioso en equipos vitales del sistema.	No existen políticas de seguridad de la información en la compañía. No aplicar u observar las políticas de seguridad de la información		

4.3.3. Identificación de riesgos

La identificación del riesgo se realiza determinando las causas, con base en los factores internos y/o externos analizados para la entidad, y que pueden afectar el logro de los objetivos. De acuerdo con la guía se definen los siguientes aspectos:

Riesgo: Representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos.

Causas (factores internos o externos): Son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

Descripción: Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

Efectos: Constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes

Tabla 4-3: Identificación del riesgo[62]

PROCESO: Interceptación de Comunicaciones telefónicas			
Objetivo: Aplicar los elementos de seguridad que garanticen la integridad y la reserva de la información, durante las actividades de interceptación de la institución.			
CAUSAS	**RIESGO**	**DESCRIPCIÓN**	**CONSECUENCIAS POTENCIALES**
✓ Intereses políticos ✓ Es más rápida la Evolución de las tecnologías que el Trámite legal de las normas. ✓ Corrupción ✓ Intereses personales ✓ Intereses de determinados grupos sociales. ✓ Herramientas de seguridad débiles. ✓ No aplicar u observar las políticas de seguridad de la información ✓ Falta de Idoneidad para el manejo de la operación. ✓ Bajas remuneración de los funcionarios según su cargo. ✓ Falta de ética profesional de los funcionarios. ✓ Inmediatez de los hechos. ✓ Desconocimiento del procedimiento ✓ Extralimitación de las funciones asignadas.	Interceptación ilegal	Omisión accidental y/o deliberada de tareas y actividades, de los procedimientos y protocolos legales relacionados con la interceptación de comunicaciones.	- Sanciones legales - Poner en riesgo la Seguridad del estado - Perdidas económicas - Pérdida de imagen de la institucionalidad - Desestabilización de Gobiernos

4.3.4. Análisis del Riesgo:

"El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, éste último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a

[62] La identificación del riesgo se realiza determinando las causas, con base en los factores internos y/o externos analizados para la entidad, y que pueden afectar el logro de los objetivos. Ibídem.

implementar... El análisis del riesgo depende de la información obtenida en la fase de identificación de riesgos"[63].

Tabla 4-4: Tabla de Probabilidad del riesgo

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en Circunstancias excepcionales.	No se ha presentado en el último año.
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en Un año
3	Posible	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de 1 vez en Cada semestre
4	Probable	Se espera que el evento ocurra en la mayoría de las circunstancias	Al menos de 2 veces por semestre
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 5 veces en el año por trimestre

La probabilidad del riesgo arrojada fue "Casi seguro", este resultado se obtuvo de la información de identificación del riesgo y la consulta hecha a los expertos del área, de interceptación telefónica de la entidad.

La siguiente tablas muestran los indicadores para la calificación del riesgo

Tabla 4-5: Tabla de Impacto

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

En Morado se resalta el indicador que indica una alarma grave en el procedimiento, A partir de este de acuerdo con la norma 31000 [36]y la guía citada, es fundamental entrar

[63] Ibídem.

a desarrollar un proceso riguroso a fin de evitar las consecuencias graves para la entidad..

Tabla 4-6: Tabla del Impacto obtenido

TIPO IMPACTO	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTROFICO (5)	TOTAL
CONFIDENCIALIDAD DE LA INFORMACIÓN				X		4,25
DE CREDIBILIDAD O IMAGEN					X	
LEGAL					X	
OPERATIVO			X			

El impacto obtenido, se encuentra en el indicador "Mayor", de la tabla 5-5. Esta calificación se procede a ubicarla en la matriz de calificación como se presenta en la siguiente tabla:

"Evaluación del Riesgo: permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad al mismo; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento"[64].

Tabla 4-7: Matriz de Calificación, Evaluación y respuesta de los Riesgos

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo baja: Asumir el riesgo
M: Zona de riesgo Moderada: Asumir el riesgo, reducir el riesgo
A: Zona de riesgo Alto: Reducir el riesgo, Evitar, Compartir o Trasferir
E: Zona de riesgo Extremo: Reducir el riesgo, Evitar, Compartir o Transferir

[64] Ibídem

De acuerdo a la clasificación, el riesgo analizado quedo en **zona E**, (Extremo)

Con una probabilidad que ocurra de cinco (5) y un impacto de cuatro (4), tratándose de un tema tan sensible para las entidades de seguridad del estado, y su impacto a la seguridad de este, se encuentra que el proceso de interceptación requiere en forma urgente, ser tratado, involucrando a todos sus actores, en particular para la entidad tratada es impresidible realizar un proceso de tratamiento del riesgo.

Tabla 4-8: Matriz de Calificación, Evaluación y respuesta de los Riesgos [39]

PROCESO: Interceptación de comunicaciones telefónicas					
OBJETIVO: Aplicar los elementos de seguridad que garanticen la integridad y la reserva de la información, durante las actividades de interceptación de la institución.					
RIESGO	**CALIFICACIÓN**		**TIPO de Impacto**	**Evaluación Zona de Riesgo**	**Medidas de Respuesta**
	Probabilidad	**Impacto**			
Interceptación Ilegal	5	4	- Confidencialidad de la información - Credibilidad o Imagen - Legal - Operativo	Zona Riesgo Extrema	Evitar, reducir, compartir o transferir el riesgo

La tabla 5-9, muestra la valoración de los controles, realizada bajo las normas 31000 [36], 27001 [38]y la guía para la administración del riesgo [37].

Tabla 4-9: Valoración de controles (Parte 1)

PROCESO: Interceptación de comunicaciones telefónicas									
OBJETIVO: Aplicar los elementos de seguridad que garanticen la integridad y la reserva de la información, durante las actividades de interceptación de la institución.									
Causas	**Control**	**TIPO**			**Valoración del control**	**Criticidad de los controles**			**Resultado Criticidad**
		P	D	C		**Integridad**	**Disponibilidad**	**Confidencialidad**	
- Intereses políticos	No existe	N/A	N/A	N/A	1	N/A	N/A	N/A	0
- Es más rápida la Evolución de las tecnologías que el Trámite legal de las normas	No existe	N/A	N/A	N/A	1	N/A	N/A	N/A	0
- Corrupción	- Código único disciplinario			X	3	0	0	0	0
	- Sistema Biométrico de registro de huella, rostro o iris.	X			2	0	1	1	2
	Circuito cerrado de televisión			X	2	0	1	1	2
- Intereses personales	No existe	N/A	N/A	N/A	1	N/A	N/A	N/A	0
- Intereses de determinados grupos sociales.	No existe	N/A	N/A	N/A	1	0	0	0	0
- Herramientas de seguridad débiles. -	Sistema Biométrico de registro de huella, rostro o iris.		X		3	0	1	1	2
	Identificar soluciones automatizadas	X			4	0	0	0	0
	Adquirir y mantener infraestructura tecnológica	X			3	1	1	N/A	2
	Garantizar la seguridad de los sistemas (Prevención, detección y corrección de Sw malicioso)	X			4	1	1	1	3
- No aplicar u observar las políticas de seguridad de la información -	Difusión de políticas al personal	x			3	1	0	0	1
	Administrar datos	x			4	1	0	0	1

P: Control preventivo. D: Control Detectivo. C: Control Correctivo

Tabla 4-10: Valoración de controles (Parte 2)

Causas	Control	TIPO			Valoración del control	Criticidad de los controles			Resultado Criticidad
		P	D	C		Inte-gridad	Disponi-bilidad	Confiden-cialidad	
- Falta de Idoneidad para el manejo de la operación. -	Personal competente y capacitado	X			3	1	0	0	1
- Bajas remuneración de los funcionarios según su cargo.	Bonificaciones	X			2	0	0	0	0
- Falta de ética profesional de los funcionarios.	- Código único disciplinario			X	2	0	0	0	0
- Inmediatez de los hechos.	Procedimientos establecidos para la interceptación de llamadas	X			2	0	0	0	0
- Desconocimiento del procedimiento	Capacitar y retroalimentar al personal	X			3	0	0	0	0
- Extralimitación de las funciones asignadas.	Manual de funciones	X			3	0	0	0	0
TOTALES					**47/19 = 2,5**	5	5	4	14 (8 de tecnología)

P: Control preventivo. D: Control Detectivo. C: Control Correctivo

Tabla 4-11: Tabla de efectividad de controles

Efectividad de los controles	Valor
No existen controles	1
Están documentados pero no se aplican	2
Están documentados se aplican y no son efectivos	3
Están documentados se aplican y son efectivos	4

Criticidad de los controles: Cuando el control cumpla los elementos de la criticidad se le da un valor de 1, lo contrario no tendrá valor, queriendo decir que el mayor valor es tres (3), efectividad en la criticidad o cero (0) el menor valor.

Conclusión y Análisis

Los controles existentes son en mayor parte preventivos, luego detectivos y en mínima parte correctivos, la ponderación de la valoración de estos, arroja un resultado de 2,47, lo que significa, que están documentados pero no se aplican.

Criticidad: En términos generales la criticidad para los controles tecnológicos, se encuentran equilibrados, en términos de Integridad, Disponibilidad y confidencialidad

Se puede observar que los controles son deficientes, dada la valoración de 2,47 esto indica que el riesgo no cambia o sale de la zona de calor. En consecuencia se mantiene en el mismo nivel, tanto en términos de probabilidad como de impacto.

Conclusión:

Se debe realizar plan de tratamiento de riesgos o matriz de riesgos.

Tabla 4-12: Nueva valoración de acuerdo a los controles identificados

PROCESO: Interceptación de comunicaciones telefónicas					
OBJETIVO: Aplicar los elementos de seguridad que garanticen la integridad y la reserva de la información, durante las actividades de interceptación de la institución.					
RIESGO	**CALIFICACIÓN**		**Tipo Impacto**	**Evaluación Zona de Riesgo**	**Medidas de Respuesta**
	Probabilidad	**Impacto**			
Interceptación Ilegal	5	4	- Confidencialidad de la información - Credibilidad o Imagen - Legal - Operativo	Zona Riesgo Extrema	Evitar, reducir, compartir o transferir el riesgo

Tabla 4-13: Mapa de riesgos (Operativos)

PROCESO: Interceptación de comunicaciones telefónicas						
OBJETIVO: Aplicar los elementos de seguridad que garanticen la integridad y la reserva de la información, durante las actividades de interceptación de la institución.						
Riesgo	**OPCIONES MANEJO**	**ACCIONES**	**ENTREGABLE**	**FECHA DE INICIO**	**FECHA FINAL**	**RESPONSABLE**
Interceptación Ilegal	Evitarlo o reducirlo	**Personal:** Diagnóstico de necesidades de capacitación y competencias del personal que participa en el proceso de interceptación telefónica	Informe ejecutivo	Enero de 2016	Diciembre de 2016	Gerente del proceso en la Entidad
	Evitarlo o reducirlo	Priorizar de acuerdo al presupuesto la necesidades que se pueden satisfacer	Propuesta de capacitación	Enero de 2016	Diciembre de 2016	Gerente del proceso en la Entidad
	Evitarlo o reducirlo	Contratar las capacitaciones y estructurar un cronograma de ejecución	Contratación Cronograma de capacitación del personal	Febrero de 2016	Diciembre de 2016	Gerente del proceso, Área administrativa en la Entidad
	Evitarlo o reducirlo	Evaluar el personal al término de la capacitación	Resultado de la evaluación	Junio y Diciembre de 2016	Diciembre de 2016	Gerente y Área de Evaluación y control proceso

Riesgo	OPCIONES MANEJO	ACCIONES	ENTREGABLE	FECHA DE INICIO	FECHA FINAL	RESPONSABLE
Interceptación Ilegal (Tecnología)	Evitar, reducir, compartir o transferir el riesgo	Asesoría para la adquisición de tecnologías de interceptación	Estudio de vigilancia tecnológica	Enero de 2016	Diciembre de 2017	- Gerente del proceso - Grupos de proyección tecnológica
	Evitar, reducir, compartir o transferir el riesgo	Construcción de un proyecto para la adquisición e implementación de nuevas tecnologías de interceptación.	Proyecto	Febrero de 2016	Abril de 2016	- Gerente del proceso Grupos de proyección tecnológica
	Evitar, reducir, compartir o transferir el riesgo	Suscribir y formular el proyecto ante el BPIN (Banco de programas y proyectos de inversión Nacional)	Aprobación del proyecto ante el ministerio	Marzo de 2016	Junio de 2016	- Gerente del proceso Área Administrativa
	Evitarlo o reducirlo	Adquirir e implementar tecnología de punta.	Puesta en marcha de la tecnología.	Año 2016	Diciembre 2016	Grupos de proyección tecnológica
	Evitarlo o reducirlo	Aplicar buenas prácticas en seguridad de la información	Toma de conciencia del personal evaluándolo sobre las buenas prácticas evaluadas.	Año 2016	Diciembre de 2016	- Gerente del proceso Funcionarios de la Unidad
	Evitarlo o reducirlo	Desarrollar e implementar un proyecto de prospectiva tecnológica permanente al interior de la institución.	Estudio de Prospectiva, a 10 años	Febrero de 2016	Diciembre de 2016	- Gerente del proceso Grupos de proyección tecnológica

4.3.5. Observaciones

El riesgo hallado de acuerdo con los resultados del mismo, también puede ser transferido a los organismos que construyen las leyes, toda vez que fortalecer estas no depende de quien tiene que ejecutar el proceso de interceptación telefónica.

Los factores de mayor incidencia para que el riesgo se encuentre en nivel catastrófico son; el factor político, el factor humano que desarrolla ejecuta y produce el proceso de interceptación y el factor tecnológico por sobrecostos y dificultad de tecnología de punta.

4.3.6. Impacto ambiental de las tecnologías de Interceptación telefónica en Colombia

Definidos los factores externos:

- ✓ Emisiones de dióxido de carbono por parte de tecnologías de interceptación.
- ✓ Disposición inadecuada de la RAEES (Residuos de aparatos eléctricos y electrónicos), porque o existen gestores adecuados.

En el análisis de riesgos, se observa que el impacto ambiental de estas tecnologías no es significativo, toda vez que no se logra consolidar como un riesgo, al no trasladarse durante el proceso de análisis de la matriz, toda vez que los equipos que utiliza con el desarrollo de últimas tecnologías, son no tangibles, esto es, son herramientas de software, que se instalan en servidores o quipos de computo de la entidad.

En cuanto a las tecnologías tácticas, no se evidencia tampoco un riesgo significativo, toda vez que corresponden a receptores y transmisores de baja potencia sin llegar a ser una amenaza para el medio ambiente.

Sin embargo es importante disponer la disposición de la RAEES, conforme a las normas establecidas para este fin, en el caso particular de la Entidad, allí existe, un procedimiento para la disposición de residuos, gerenciado por la unidad tecnológica de la entidad.

5. Conclusiones y recomendaciones

5.1. Conclusiones

1. La interceptación telefónica, se ha convertido en una de las herramientas más usadas en forma generalizada por diferentes países en el mundo para conocer información sensible que permita evitar la comisión de delitos de alto impacto a su Seguridad Nacional. Esto ha ocasionado que diferentes sectores de la sociedad se pronuncien al respecto solicitando ante los organismos internacionales de Derechos humanos, la necesidad de poner control al uso de la interceptación telefónica.

2. Existe una serie de normas y convenios de tipo internacional, entre diferentes países, con el fin de tener un apoyo mutuo consistente en compartir información estratégica, así como el uso de herramientas tecnológicas, para la lucha contra el terrorismo, la delincuencia organizada a nivel Nacional e internacional, la lucha antidrogas y la prevención de delitos de alto impacto.

3. El uso de la interceptación telefónica, bien utilizada ha dado grandes resultados a nivel internacional y nacional, en el caso colombiano, la lucha contra grupos terroristas, como las Farc, también han evitado la comisión de delitos de alto impacto como la detonación de bombas en las principales ciudades, por otra parte se han logrado someter a la justicia individuos que le han hecho daño a la sociedad y al País. En estos casos la interceptación ha jugado un papel importante como instrumentos para obtener información que ha conducido a la captura de estas personas.

4. El uso de la Interceptación telefónica, también ha dado lugar a escándalos por parte de los organismos del estado, en la última década, su protagonismos fue determinante para que se realizaran reformas de orden institucional y normativo, así como la creación de nueva regulación a fin de poner un control al uso de esta, por quienes cumplen esta función en el estado colombiano.

5. Con el desarrollo de este trabajo se hicieron aportes en el área regulatoria, mediante la participación en la elaboración de una propuesta en materia de interceptación telefónica, a través de una de las unidades de la entidad que se

encarga de realizar y ejecutar estas tareas, de esta forma se logra realizar una reforma al código de procedimiento penal Articulo 235, de la misma forma a partir de los planteamientos del trabajo, estos sirven como insumos para la creación del decreto 1704, que incluye de alguna forma, apartes de la propuesta. También en la ley de inteligencia y contrainteligencia se refleja el desarrollo de este trabajo, al incluirse unos apartes en esta norma.

6. En lo técnico, se evidencio, que cada día hay desarrollo masificado de nuevas tecnologías y herramientas de interceptación, cada vez más poderosas y de mayor capacidad para obtener y procesar información de las redes de telecomunicaciones, tanto de voz como de datos. Un inconveniente hacia la sociedad es que muchas de estas tecnologías son intrusivas, vulnerando de manera directa los derechos fundamentales como: Derecho a la intimidad personal y comunicación privada (Artículo 15 de la Constitución Política de Colombia), Derecho a la libre expresión (Artículo 44 de la Constitución) [2].

7. En Colombia se evidencia un debilidad en las normas para el control de la interceptación telefónica y la adquisición, producción y uso de las herramientas tecnológicas usadas para esta práctica, de la misma forma las entidades de seguridad del estado que tienen a su cargo estas funciones, presenta fallas y debilidades en el proceso. Esto lo demuestra casos como el de la sala “Andrómeda”.

8. El proceso de interceptación, presenta un riesgo calificado en estado crítico “La interceptación ilegal”, el cual debe su grado de criticidad a diferentes causales internas y externas, como se evidencia en el análisis de riesgos y calificación del riesgo, desarrollado a través de la matriz de riesgos. Por lo cual se hace necesario realizar un plan de mejoramiento en la entidad que tiene esta función como misión institucional por parte del estado, en lo operativo y tecnológico.

5.2. Recomendaciones

1. Crear un grupo de investigación orientado a desarrollar herramientas de software que permita el seguimiento de determinados tipos de datos en la red, esto es una especia de “policía virtual”. Para ello es imprescindible buscar la asesoría y/o acuerdos o convenios con empresas de alto nivel en desarrollo de software en el mundo, entre las cuales se deben considerar aquellos proveedores de tecnologías de interceptación con los cuales Colombia ha adquirido sus más resientes sistemas.

2. Las tecnologías (hardware y software), adquiridas por Colombia, le han costado al País al menos más de US 100´000.000, estas tecnologías se utilizan mientras son compatibles con los protocolos de comunicaciones, pero una vez se renuevan las tecnologías, estos equipos quedan inservibles, y se deben realizar nuevas inversiones, así quedó demostrado en el estudio de las herramientas tecnológicas, entonces qué hacer? Se debe dar una tendencia hacia el uso de software y solicitar a los proveedores que debe ser código abierto, y mediante convenios establecer las reglas que posibiliten su actualización por personal entrenado por el fabricante a fin de poder escalar estos programas a los nuevos protocolos. Siempre que sea viable.

3. El artículo 44 de la ley 1621, establece la obligación de las empresas de comunicaciones de suministrar información de sus suscriptores a los organismos de seguridad del estado y que deben retener los datos de estos por cinco (05) años. En este sentido se requiere precisar de qué forma se van a almacenar estos datos, sobre que tecnología y mediante que controles legales se debe realizar, así mismo se debe contar con la infraestructura para su retención, la cual deberá preverse antes de iniciar el proceso. En cuanto a la retención de información, la norma no es clara si también se incluye información de las comunicaciones de los suscriptores, lo que requiere normalizar y establecer las causales para esto.

6. Bibliografía

[1] S. D. &. R. M. Federman, *Seguridad Nacional: El realismo y sus contradicciones, Desafíos,* Universidad del Rosario, 2006.

[2] C. d. l. República, «Titulo 1; De los Principios fundamentales, articulo 2. Título II; de los derechos, las Garantías y los deberes, articulo 15.,» de *Constitución Política de Colombia del 1991*.

[3] U. (. I. d. Telecomunicaciones), *Guía de ciberseguridad para los países en desarrollo,* 2007., p. 96 de 165.

[4] Contraloría de Bogotá, «Informe de la Contraloría de Bogotá, No. 35000- 3462,» 30 de enero de 2006.

[5] «Asociación de Profesor de derecho Penal .Articulo "Legalidad de la interceptacion de comunicaciones en Colombia ",» [En línea]. Available: www.larepublica,com.co. [Último acceso: 20 Octubre 2009].

[6] «Inteligencia , Espionaje y Servicio Secretos,» phpBB Limited , [En línea]. Available: http://www.intelpage.info/forum/search.php?keywords.

[7] F. o. A. Scientists, «Intelligence Resource Program,» Federation of America Scientists, 2006. [En línea]. Available: http://fas.org/irp/index.html.

[8] J. R. v. I. M. Álvarez, «Sentencia T-1319, Corte Constitucional,» 7 Diciembre 2001. [En línea]. Available: <http://www.corteconstitucional.gov.co/relatoria/2001/t-1319-01.htm>.

[9] Rodrigo Uprimny Yepes Bogotá, 2006, «Bloque de constitucionalidad, derechos humanos y nuevo procedimiento penal, Escuela Judicial Lara Bonilla, Consejo Superior de la Judicatura,» 2006. [En línea].

[10] C. I. d. D. Humanos, *Sentencia,Serie C No 200,* 2009.

[11] M. M. Daniel., *Informantes y técnicas de Investigación encubiertas .Análisis constitucional y proceso penal.,* p. 368.

[12] Directiva 2006/24/CE del parlamento europeo y del consejo , 15 Marzo 2006. [En línea]. Available: https://www.boe.es/doue/2006/105/L00054-00063.pdf.

[13] «ratado del Atlántico Norte, sobre Cooperación y Seguridad de Información,» 25 Junio 2013 . [En línea]. Available: http://apw.cancilleria.gov.co/tratados/SitePages/VerTratados.aspx?.

[14] UIT, «Recomendacion -UIT -T Serie Y 2201,» Abril 2007. [En línea]. Available: http://www.itu.int/es/Pages/default.aspx.

[15] Parlamento Europeo y Consejo , *Ley 34 ,De servicios de la sociedad de la información y de comercio electrónico,* España , 2002.

[16] Centro Nacional de Inteligencia , *Trata acerca de los servicios de inteligencia eficaces especializados y moderados , capaces de afrontar los nuevos retos del actual escenario nacional e internacional,* España , 2002 .

[17] K. R. Juan Camilo Rivera, *Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamnetales en Colombia,* 2015.

[18] C. d. l. República, «Ley 137 de 1994.,» [En línea]. Available: http://wsp.presidencia.gov.co/Normativa/Leyes.

[19] comunicaciones, Ministerio de tecnologías de la información y las, *Decreto No.1704,* 2012.

[20] P. d. l. Republica, *Decreto 857,* 2014.

[21] D. OEA, «Informe anual de la Comisión Interamericana de Derechos Humanos 2009,Capítulo IV, párr. 137, y 13,» 2009. [En línea]. Available: http://www.cidh.oas.org/annualrep/2009sp/cap.4Colo.09.sp.htm.

[22] Congreso de la Republica, *[18] Ley 1288 de 2009. “Se expiden normas para fortalecer el marco legal".*

[23] Comisión interamericana de derechos humanos - organizacion de los estados americanos , «informe anual de la comisión interamericana de derechos humanos,» 2009.

[24] Americanos, comisión interamericana de derechos humanos -organizacion de los estados, «informe anual de la comisión interamericana de derechos humanos - capitulo iv,» 2009.

[25] Presidencia de la Republica , *Decreto 075 de 2006,* 2006 .

[26] Congreso de la Republica , *Ley 1273 de 2009. "Modifica el código penal, crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos.*

[27] C. d. l. República, *Ley 906,* 2004.

[28] E. NIZKOR, «Texto de la sentencia en el caso de las ecuchas ilegals del DAS,» 30 Noviembre 2012. [En línea]. Available: http://www.derechos.org/nizkor/colombia/doc/das299.html#259.

[29] «PEN.LINK,»Pen-Link,Ltd,2015.[Enlínea].Available: https://www.penlink.com/Home/tabid/37/Default.aspx.

[30] S. S. Surveillance, *Law and Order in Colombia,* 2015.

[31] M. C. Restrepo, «La Republica ,Verint Systems planea poner una oficina en Colombia,» 18 Junio 2014. [En línea]. Available: http://www.larepublica.co/verint-systems-planea-poner-una-oficina-en-colombia,.

[32] A. U. A. S. .. a. S. I. Globally, «Homcept Solutions Limited,» [En línea]. Available: http://www.komcept.com/products.php.

[33] «Contratos por más de US 35 millones para renovar salas de interceptación,» Caracol Radio , 25 Abril 2014. [En línea]. Available: http://caracol.com.co/radio/2014/04/25/judicial/1398407940_194095.html.

[34] «NICE Systems Ltd.,» [En línea]. Available: http://www.nice.com/.

[35] C. d. l. república, «Ley 1098 de 2006,» 8 Noviembre 2006. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004_pr005.html.

[36] N. T. C. Icontec, *NTC-ISO 31000. Gestión del riesgo, principios y directrices,* 2009.

[37] D. A. d. l. F. P. D. d. C. I. y. R. d. T. Bogotá., *Guía para la Administración del Riesgo,* 4ta ed., 2011.

[38] E. Internacional, *ISO 2700 Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos,* 1ra ed., 2005.

[39] D. A. d. l. F. P. D. d. C. I. y. R. d. T. Guía para la Administración del Riesgo, Bogota : 2011.

6.1. Bibliografía Adicional

- FARFAN M, francisco, La interceptación de comunicaciones electrónicas.
- LUCAS K. Estados Unidos en guerra, del miedo a la libertad vigilada. Editorial Abya Yala. 1ra ed. Quito Ecuador. 2001.
- DOMSCHEIT- Berg, Daniel. Dentro de Wikileaks. 1ra ed. Editorial nomos impresores. Colombia 2011.
- GARCIA M. Nacho, Libertad Vigilada, el espionaje de las comunicaciones. 1ra edición. Editorial Domingraf. S.L. Barcelona España. 2003.
- CARBONE C. Alberto. Grabaciones, escuchas telefónicas y filmaciones como medios de prueba. 1ra edición. Editorial Rubinzal-Culzoni Editores. Buenos Aires. 2005. 2da Edición. Editorial AD-HOC S.R.L. Buenos Aires. 2001.
- Decreto 1900 de 1990., Agosto 19. “Por el cual se reforman las normas y estatutos que regulan las actividades y servicios de telecomunicaciones y afines".
- La admisibilidad de la prueba electrónica ante los tribunales: luchando contra los delitos tecnológicos_2005. www.cybex.es. UIT.
- Ley federal de Telecomunicaciones de 1995. (México).
- Acta del 05/09/2001 - Edición provisional ECHELON A5-0264/2001

- "Surveillance, Search or Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States"; Office of the Privacy Commissioner of Canada.

- Efficient File Hash Identifier Computation, Número de Patente: US2009089337 (A1). Número de Publicación: Fecha de publicación: 2009-04-02. Inventor: Perlin Eric C [Us]; Pudipeddi Ravisankar V [Us].

- Phishing Activity Trends Report 2nd Half / 2008, editing completed by Ronnie Manning, Mynt Public Relations, www.apwg.org.

- Método para monitorear un sistema de comunicaciones. Número de patente: US005542120A , Fecha de publicación: 30-07-1996. Inventor: Anthony J. Smith, Peter J. Myers.

- GONZALEZ S. Karla Verónica. La inteligencia estratégica.